POINTER

Journal of the
Singapore Armed Forces

Vol. 28 No. 3 [2002]

V28N3

Editorial

We are pleased to announce that for this issue (July - September), the Editorial team has adopted an SAF-centric theme. We have selected articles which look at various aspects of the SAF, such as in training, learning, professionalism or technological advances. Included also in this issue are three of the top ten CDF Essay Competition entries which could not be published in the last issue due to space constraints. Tehse three essays are also SAF-related. This issue includes a sub-theme on a very current topic - terrorism. We present three essays which address different aspects of terrorism.

The issue kicks off with a lead article by COL Jimmy Tan and MAJ Irvin Lim. *From Terror Fallout to Terra Firma - Convergent Focus on Strengthening Homeland Security* points out that traditional approaches to tackling conventional aggression will no longer suffice when faced with the rising terrorist threat. The authors stress the need for a clear national security strategy and propose some principles for homeland security that take on a "convergent focus", a coordinated and integrated approach by all security agencies.

LTC Richard Pereira argues in his essay, *The SAFL From Training to Learning Effectiveness* that learning in the SAF should be strategic and geared towards enhancing fighting effectiveness, and elucidates on how such a framework of learning in the SAF can be established. *Riding the Crest of RMA Massive Systemic Shock - Can We Do It?* by MAJ Roland Ng, examines how the SAF can ride on the crest of technological advances to induce a "massive Systemic Shock" (brought about by the interaction of separate technical components acting together as a synergized whole) on the enemy's systems to gain combat victory.

In *A Culture of Transformational Change - Strategies for the SAF*, MAJ Seet Pi Shen argues that fundamental changes are need for today's military to operate effectively in a world of continuous changes. He proposes five strategies to help the SAF to adapt to such a culture of change. Manpower policies in the SAF, CPT Lim Ann Nee opines, have gradually shifted toward more commercial-like practices, with emphasis on monetary rewards. In her essay *The Professional Soldier*, she contends that while extrinsic rewards are important, SAF servicemen must understand the meaning behind military service, and stresses the need for the SAF leadership to inculcate the traditional core values in its people.

In *Cyber Terrorism, An Emerging Security Threat of the New Millennium*, CPT Ow Kim Meng highlights that terrorism can take on other forms beyond physical violence. He examines the vulnerabilities of key infrastructure to cyber-terrorism and the necessary security measures ot be taken to combat this threat. *The Motivations and Methods of a Terrorist* goes beyond terrorist acts to delve into the causes and motivations of a terrorist. The author, MAJ (NS) (DR) Aaron Chia also discusses the strategies, tactics and weapons used by terrorists.

We wrap up this issue with an article on the use of force in self defence. In her essay, *When States May Lawfully Resort to Armed Force*, Ms Ong Yen Nee examines this issue under the framework of the United Nations charter and discusses how a broad interpretation of the UN articles is often used by states to justify their use of force.

We are pleased that the Singapore Civil Defence Force had recently subscribed to *POINTER*, and asked for it to be distributed to all their stations. We have received positive feedback from one of the readers, and we would like to share this with you. We have published this under the "Letter to the Editor" page. We urge readers to write to the Editor to give their views on any of the articles published and we hope that this will stimilate discussion and debate among our readers. We also encourage readers to visit our web-site at http://www.mindef.gov.sg/safti. For those who have access to MINDEF Intranet, we can be found under the SAFTI MI homepage. We are upgrading our web-site and we hope to inform you of the changes soon.

Finally, a gentle reminder that the CDF Essay Competition-2002 will close on 31 Dec 2002. Do send in your entries before then.

Editor, *POINTER*

Letter to the Editor

I have just received the January March 2002 edition of *POINTER*.

After reading some of the articles, my overall view is that the publication is well researched and well written. I say this because I liked the simple straight-to-the-point story-telling.

One article that really struck me was the Battle of Pasir Panjang Revisited. I never knew of the battle of Pasir Panjang and I am glad I do now. Set against the backdrop of PM Goh's "Stayers" or "Quitters" contrast, the battle seems so much more important then and now. It would have been good if the story of the Battle of Pasir Panjang and the brave Malay Regiment was narrated during the National Day Rally.

Kudos to the whole Editorial Board. I am looking forward to the next issue.

CPT Nicholas Lee

OC, Woodlands Fire Station, 4th CD Div, SCDF

Editor's note:

We thank the writer for his letter and we are heartened by the positive feedback. We strive to present articles which are relevant and which stimulate thought and provoke discussion. We hope our readers will continue to enjoy our articles.

CDF Essay Competition 2002

***POINTER* is pleased to announce the 16th Annual Chief of Defence Force Essay Competition. The competition aims to encourage SAF officers to conduct research on professional and military-related issues relevant to the SAF to enable our Officer Corps to move towards excellence.**

Rules

1. The Competition is open to all SAF officers and Warrant Officers (Regulars, NUSAF, NSF, NSmen and Officer Cadets).

2. Entries may be submitted as an individual or group effort, however the entries must be unpublished work.

3. The essays should be between 2,000 to 4,000 words, typewritten, double-spaced on A4-size paper with all pages numbered.

4. A separate cover sheet with the following details should be included: essay title, writer's/writers' name(s), sex, rank, educational qualifications, Service status, unit, home address, contact number and word count. The writer's/writers' name(s) should not appear in the main essay. The essay title should be repeated on the first page of the essay.

5. All entries must include detailed footnotes/endnotes and a bibliography.

6. The closing date of the competition is **31 Dec 2002**. Entries which do not comply with any of the competition rules will be disqualified.

7. The essays will be assessed in confidence by an independent panel of judges. No appeals will be entertained. Results of the competition will be announced in May 2003.

8. The editorial board reserves the right to edit essays selected for publication.

9. For further information, please call the Editor at 799-7410 or Assistant Editor at 799-7409 or e-mail them at the SAFTI MI HQ address.

Topics

10. Entries may be submitted on any of the following subjects:

- Military strategy and tactics
- SAF doctrinal development and concepts
- Professionalism and leadership in the military
- Military ethics, values and *esprit de corps*
- Military campaigns or history and their relevance to the SAF
- Personal experiences in combat operations or overseas training
- Administration, rescue operations and decision-making during a crisis

- Regional geopolitics and strategic issues
- Military and defence technology

Prizes

11. Prizes will be awarded as follows:

- First prize $1,500 and a plaque
- Second prize $1,000 and a plaque
- Third prize $500 and a plaque
- 7 Merit Awards $300 each and a plaque
- 10 Commendation Awards $300 each

From Terror Fallout To Terra Firma Convergent Focus On Strengthening Homeland Security

By COL Jimmy Tan Cheng Yaw & MAJ Irvin Lim Fang Jau

"It is not possible for us to deal with these new threats with the same type of structure and capabilities we had in the past It does not make sense for us to pretend that these threats are not there. They are there, and we have to guard against them At the same time, we should not let these threats disrupt our way of life. "

Dr Tony Tan, DPM and Minister of Defence, 6 Jan 2002[1]

"Homefront security must be the shared responsibility of every Singaporean."

Mr Wong Kan Seng, Minister of Home Affairs, 17 May 2002[2]

Introduction: Strategic Insecurity

The global security climate took a sudden nose-dive from one of post-Cold War euphoric "New World"Order to one of strategic insecurity - after Sep 11. The dark plumes from the collapsed WTC buildings subsequently gathered to form war clouds over Afghanistan and cast a pall of dread over many other parts of the world. The geopolitical implications continue to play out beyond Central Asia and the Middle East with the potential complication of an event involving the diabolical use of Weapons of Mass Destruction. With such a dim prospect in mind, the war on global terrorism is clearly not just an American one.

Terrorism has in fact taken on a catastrophic and strategic dimension, well beyond the sharp surrealism of the WTC strikes at the heart of America. Terror operations are no longer waged solely by disaffected groups and individuals on a local scale with limited goals, but by radicalised groups operating through well-funded global networks of cells with grander grotesque agendas. The new global terrorism is not ad hoc or tactical in nature but highly synchronised, self-organising and strategic in its "global media-spectacular" objectives. Many would-be terrorists with malleable domestic agendas appear ready to rise to the battle-call. Many of them also appear to draw inspiration from the ready-made Al Qaeda discourse of unmitigated violence. In fact, many are also being franchised through its "pyramid" network of global support and sympathisers. The new enemy operates clandestinely through secure cells amongst indigenous populations. Recent Pakistani intelligence reports indicate that the Al Qaeda network has made plans for a world-wide suicide-bombing offensive against the US and its allies. Such sinister threats have already manifested in the acts like those of the suicide bomber who killed 15 people, including 11 French nationals, in Karachi in May 2002. Another fatal attack occurred barely a month later on 14 June 02 when a bomb explosion outside the US Consulate-General's office in Karachi killed 12 people.

Even after the dust has settled on the US war in Afghanistan, with possibly another one kicked up in the Persian Gulf again, it is likely that the global war on terrorism will continue for some time and with far-reaching ramifications. The anticipated global and sustained nature of warfare against terrorism requires a major rethink of the way national security is to be attained and preserved. For many countries, security now begins, first and foremost, at home. As one writer puts it: "When war comes home, so must war strategy."[3] *The same keen focus on homeland security applies acutely to a small and open city-state like Singapore.*

Taking Stock of the Rising Tide of Terror

Like many countries, Singapore has responded to the new threats and geopolitical insecurities by tightening and beefing up our military defence and homefront security apparatus. We have also judiciously reviewed and kept our contingency plans warm to deal with any sudden deterioration in our external and internal security environment. But whatever we do, Singapore cannot expect to escape entirely from the negative spill-over effects of global terrorism. Being a small and porous society plugged right into the global economy, Singapore's small size, the open nature of our economy, and our fluid geostrategic environment make us an attractive target. We must therefore be constantly vigilant with resolute zero-tolerance for terrorism-related activities. The challenges to our border and internal security are compounded by the fact that Singapore is both a busy international air hub and sea hub with a highly mobile population. Every day, hundreds and thousands of people and goods move in and out of Singapore. It is clear that increased security comes at a high price, and we must find a balance between the many competing economic, social and security demands while safeguarding our vital infrastructure and interests.

The preventive arrests of 13 *Jemaah Islamiyah* (JI) cell members, who had plotted to bomb American interests in Singapore in late 2001, brought the uncomfortable truth of the problem right into the psyche of many Singaporeans. They had planned to make up to seven truck bombs from 21 tonnes of ammonium nitrate to blow up the US embassy and other American targets in Singapore. Plans were also afoot to hijack an airliner within the region and crash it into Singapore's Changi International Airport. Fortunately, they were discovered before they could do any damage. We have also had our fair share of anthrax scares, bomb hoaxes, plane hijack warnings and veiled threats with little signs of attribution. Recent revelations of a second wave of preventive arrests in August 2002 by Singapore's Internal Security Department of 21 Singaporeans for terrorism-related activities highlight the extent and penetration of the threat.[4]Despite our best efforts and intentions, we remain vulnerable to rogue threats that roam at large and loom in the shadows. The presence of US interests in Singapore and our open support of the US-led war against terrorism make us, like many countries, a target by association. To be sure, our security agencies will not let-up in efforts to ensure Singapore remains one of the safest countries in the world. They will continue to lessen our attractiveness and vulnerabilities as a target with a matching higher visibility deterrence posture and enhanced early warning through full-spectrum vigilance. This can help to mitigate the fear and manage uncertainty somewhat.

Indeed, the point well made by many commentators about dealing with uncertainty is not trying to predict the future. Instead, it is about framing new mindsets, developing unified organisation and putting in place responsive capabilities to deal with a range of threat scenarios. There is no single-line approach to managing uncertainty. Straight line-thinking goes out the window now that the terror of complexity and chaos threaten to shatter more than mindsets. The challenge will be to have the right strategies, policies and capabilities that are robust enough to operate effectively across a range of possible futures. In dealing with strategic complexity, *strategic convergence* of a nation's mindset, resources and capabilities appear to be the key imperatives. Before outlining some of the measures Singapore has taken, it may be useful to quickly outline the new threat context.

New Threat Context

Global terrorism appears to have sunk deep roots into many countries in Asia and around the world. Although terrorism is not a new phenomenon to Southeast Asia, they have, until recently, been largely isolated and often unrelated; albeit not regionally or globally networked. Security analyst reports indicate that Asian terrorism groups have seen an increase in numbers over the past five years, and the recent exposé of terrorist networks in several Southeast countries has led some to brand the region as a second front in the fight against terrorism. Such a disturbing development coupled with religious extremism represent highly undesirable underlying trends that must be checked lest they cause long-term disruption; particularly if the local governments are unable *or* prevaricate on curtailing the growth of extremist and obscurantist groups purveying violence. Whether politically exploited or left entirely on their own volition, such disparate groups can initiate damaging hostile actions despite their seemingly modest resources. The danger for many states faced with the threat right at their doorsteps and within their homeland has become

more real now than remote. It cannot be underestimated. Any mass casualty terrorism attacks emanating from neighbouring/domestic sources or those further afield impacting on our shores will seriously damage the region's peace, social stability and business confidence. The very survival and integrity of nation-states may come under grave threat. This has been well-acknowledged by all countries in the region, with stepped up bilateral and international cooperation. At their recent meeting on 17 May 02, senior officials from the ten ASEAN nations agreed that closer cooperation was needed to counter terrorism. A statement issued at the end of the meeting stressed that ASEAN would give priority to transnational crimes such as terrorism, arms smuggling, piracy, cyber crime, money-laundering and the trafficking of women and children. Following up quickly on the statement, the group has since concluded another important agreement the ASEAN-United States of America Joint Declaration for Cooperation to Combat International Terrorism on 1 August 2002. Such intra and extra-regional efforts highlight some of the serious multilateral inroads that have been made.

For all intents and purposes, the world post 9-11 is caught up in more than a crisis. It would not be hyperbole to say that many countries in the world are now in a general state of Low Intensity Conflict (LIC) and cannot afford to let their guard down for a moment. Low Intensity Conflict denotes a condition of irregular and interminable warfare waged across a broadfront of a nation's domains; from physical/cyber attacks and economic sabotage to social disruption and psychological dislocation. And it can persist for long periods from troubled peace to hot war. It follows then that, full-spectrum response to a LIC scenario means that the operational readiness posture of our security agencies must fit a "pulse-and- plateau"[5] profile, rather than the "ramp-and-spike"[6] profile of conventional threat scenarios. But try as some countries might, there is no*Maginot Line* or *magic bullet* when dealing with the LIC of global terrorism. This new type of Low Intensity Conflict can have disproportionately devastating effects through the sheer cunning of asymmetry and suicidal surprise. It is a threat that has no qualms about the cynical use of civilian infrastructure to attack civilian targets. In sum, it is aimed at disrupting daily life by instilling chronic public fear. It therefore demands a fundamentally new way of thinking and organising for preserving our national security. Conventional national security mechanisms, often inter-state in orientation and episodic in operation, are not well-designed to be responsive enough to deal with the new threat posed by catastrophic terrorism, waged by non-state actors, in a sustained and strategic manner.

There is now a blurring of traditional notions of external and internal defence. The boundaries between war and peace have also been clouded by the LIC of global terrorism. The key impact of such blurring will be in the redefining civil-military security functions as well as converging public-private interests to overcome the disparate nature and magnitude of potential threats. Such threats now effortlessly traverse the realms of physical, psychological and cyber space. The threat envelope and target spectrum has now widened considerably and it would be impossible to guard all gateways or angles. Some even go so far as to argue that the search for "foolproof" Homeland Security breeds Homeland insecurity, especially when not enough is done to design systems that fail smartly.[7] Quite apart from the obvious challenges ahead, it is clear that we will need to prioritise where we intend to commit resources after a circumspect survey of the most credible threat vectors and weak links throughout the national infrastructure.

To be sure, conventional security frames of references and operations designed for state defence focused on an external state's military aggression will now have to be augmented. The Sep 11 attacks do not fundamentally change the need for a strategy of deterrence and for a strong defence capability, especially for a small country like Singapore. However, the traditional focus on conventional aggression by an identifiable state adversary will not suffice when one's homeland is exposed to the global terrorist threat which is difficult to screen-out or pin-down. While diplomacy backed by a strong deterrence capability will still form the bedrock of our national security policy, homeland defence must now be looked at with new lenses and tackled with fresh ideas.

Some Organising Principles for Homeland Security

- ### Close Civil-Military & Public-Private Partnerships

  As French Judge Jean-Louis Bruguière, a key transnational terrorism crime fighter and expert on the Al Qaeda network, had put it: "Coordination is more effective than competition".[8] Civil and military

agencies must now quickly come to a consensus on the threats "out there and in here" in order to converge on the common space of close systemic coordination. Bureaucratic barriers need to be removed and turf wars avoided. The military brings to the table of inter-agency cooperation, a big plate of manpower, logistical resources, expertise and capabilities (Intelligence, Information, Aviation, Maritime *et al*) that can help augment the capability envelope of the civil security enforcement agencies. Private commercial entities will also have a bigger role to play in boosting homeland security especially when terrorists gun for soft targets commercial infrastructure, public spaces, transport and high density urban population centres - besides traditional hard targets like government buildings and assets. The onus is now on private entities and public agencies to establish clear mechanisms for crisis and consequence management, in order to respond effectively and minimise disruptions when attacks occur. Footing the costs and burden-sharing will be a joint public-private affair. In a similar vein, it is envisaged that greater public communication on joint national security education activities will be important, as both public agencies and private entities forge new partnerships and acknowledge their common stakes in preserving a climate of peace, security and stability.

- ## Integration of Effort

The new threats now require a greater degree of intelligence and operational integration to sustain a level of higher alertness and operational responsiveness. This calls for a greater integration of effort in order to fight and win this new type of conflict decisively on home ground. Integration of effort allows for enhanced real-time and round-the-clock Intelligence-Operations co-ordination. For example, the formation of Homeland Security mechanisms to achieve integration of operational command both horizontally and vertically throughout a county's decision-making structure, would serve to foster policy-operations-intelligence integration, and help determine the key capabilities to be developed to plug any gaps in the national security system. This can then lead to better exploitation of the relevant emergent technologies, as well as initiate research and development into new capabilities for military and homefront agencies.

- ## Seamless Transition from Peacetime to War

Integration of effort will also enable the seamless transition of disparate national agencies from troubled peace to hot war with minimal disruption and in a co-ordinated manner with strategic oversight. Tighter civil-military co-ordination and integration at both the policy and operational levels will be critical. The military's role in homeland defence will have to be reviewed and critical changes made to existing national command structures and civil-military organisation to facilitate its heightened responsibilities to deal with the spectrum of threats. To overcome global terrorism, war-fighting and crime-fighting must now go hand in hand. In addition, terrorism is clearly not just a homeland security issue for homefront agencies to tackle. It is also a force protection issue where the military already has a clear role and broad scope for involvement. Military force protection issues will now increasingly figure in the forefront of military planning. The challenge will be in integrating air and sea defence, and cyber defence with other components of homeland security. But the military must guard against overreach. In other words, combat readiness must not be eroded as the military takes on more responsibilities on the homefront and stretches its resources to augment the civil security agencies and national instruments of power.

- ## Clear and Concerted National Security Strategies

In order to stand up effectively against the new threat over the longer term, security and civil ministries and agencies must work even more closely in a concerted national security effort. Turf issues while at times unavoidable, should not be allowed to fester and prevent systemic co-operation. Dialogue, trust and understanding will have to be genuinely fostered in order to initiate and develop new homeland security capabilities to tackle the multifarious threats confronting a nation in the immediate and long-term. But before these can be done in a focused yet holistic manner, there is a pressing need for consensus to define national security strategies that will better

frame, prioritise and co-ordinate often disparate national security efforts. Strategies can no longer afford to be implemented and reviewed piece-meal. They must instead be reviewed constantly and comprehensively as part of a fluid continuum. The formulation of a national security masterplan or multi-year blueprint to provide policy oversight of all key national security initiatives and programmes will be crucial for driving the strategic process along.

A clear national security strategy would also augment a well-developed conventional defence strategy in an asymmetric era where war can no longer be easily contemplated and neatly conducted according to text-book manoeuvres, predicated on short and decisive victories. Any conventional war or period of tension that we can be expected to face in the future will in all probability be waged along the entire spectrum of conflict from troubled peace to hot war; though not necessarily sequentially but simultaneously. Such a war will not have a clear or easy end in sight. This is the harsh reality we must face against shadowy enemies state-sponsored or otherwise. Such enemies are not readily cornered, easily cowered, or reasonably dictated to by conventional logic premised on force of arms or cost-benefit calculus. The new terrorists are fueled by a radical religious ideology that is more intent on smashing rather than sitting at the negotiating table. Thomas Friedman has referred to them as "undeterrables".[9] Described by another analyst as "punishment terrorism", the attacks of the new terrorism are consciously committed to punish a perceived "wrong-doer", who may be a State, an organisation, group or individual. It is retributive in nature and does not have any other objective or demand to be achieved beyond the act of retribution. It is the use of terrorism as a weapon to give vent to anger and not necessarily to achieve any strategic objective or tactical demand in every instance.[10] While old-style terrorists often have a clear political goal to direct their message through often isolated acts of violence and political ransom like kidnapping, the new-age terrorists, of the Al Qaeda mould, appear more intent on making many heads roll in addition to grabbing the headlines. Mass murder and mayhem *is* the mass media message.

Groundwork for the New National Security Paradigm

Well before 11 Sep, we had already put in place an integrated national command structure that provides strategic policy oversight of our national security apparatus and operations to deal with unconventional threats. The *Security Policy Review Committee* (SPRC) made up of ministers from the key security ministries with a keen internal focus and external orientation ie. Defence, Home Affairs and Foreign Affairs. It "actively drive[s]" the build up of required capabilities and infrastructure to protect the Singapore homeland.[11] Close support is also garnered from the other national ministries on specific overlapping issues requiring special expertise eg. Health and Environment. We have also spent more than a decade building up a well-oiled Total Defence mechanism. One of the key lessons learnt from our recent experience with the national security milieu post 9-11 is the importance of better synergy and orchestration of policy coordination, strategy development, intelligence dissemination and security operations by focusing all the instruments of national power at our disposal. Towards this end, the *National Security Secretariat*(NSS) an "operationally-oriented"[12] inter-agency outfit - assumes the lead role at the strategic level in co-ordinating and integrating inter-agency efforts to build-up national resilience against threats posed by terrorism, as part of the enhanced homeland security architecture. The following critical areas below have been identified and are being holistically addressed. They also represent our new strategy-driven efforts, to ensure that Singapore continues to surmount the new security challenges that have emerged:

- ## Tighter Intelligence and Operations Integration

Since 11 Sep, Singapore's security agencies have focused significantly more resources on monitoring potential terrorist threats. To prevent fatal blind-spots, it is clear that hard arsenals alone will not be enough to tackle the new threats. We need also to focus on building sharp yet "soft capabilities" like integrated deep-cover HUMINT to penetrate terrorist cells, where possible. In addition, inter-intel agency linkages for more accurate threat/risk assessments to cue appropriate operational responses will also need to be strengthened. New mechanisms for pooling existing expertise and developing new knowledge on terrorism, with the corollary setting-up of a central

database can help build up intelligence coverage of terrorist groups for counter-terrorism purposes. Such institutional convergence will also enhance Int-Ops integration at the operational levels to enable timely and appropriate responses to alerts. The *Joint Counter Terrorism Centre*(JCTC) has been set-up to serve as the central coordinating intelligence agency to integrate the activities of the country's various intelligence services, and be the main contact point with foreign intelligence agencies. Other new outfits like the *Homefront Security Centre*(HSC) have also been set-up under the Ministry Home Affairs to work closely with their SAF and JCTC partners to oversee joint security operations and exercises to test operational responses to terrorism and other security threats on the homefront. The formation of a "scalable" *National Security Task Force* (NSTF) as an interagency body to coordinate operational response to security threats is another important example.[13] Such new outfits complement and strengthen extant structures like the National Emergency System (NEST) for ensuring civil/economic security during civil emergencies, and the Executive Group (EG) in leading the management of civil security/emergency situations like hijack, bomb explosion, terrorist sabotage or civil disaster.[14] The new outfits are not meant to create additional hierarchical layers of bureaucratic snafu. Instead they generate important new interagency nodes that will transmit greater seamless synergy throughout our entire national security network by reducing institutional stove-pipes.

- ## Closer Civil-Military Interface and Public-Private Cooperation

Over the past few years, the various security ministries and agencies of Singapore have developed the healthy habit of close interactions and consultations from the policy level down to the agency/operational levels. The close working rapport can be seen in the various national security initiatives ranging from enhancing our critical infrastructure to resource protection. The SAF and Home Team agencies have also jointly developed and fine-tuned operational mechanisms to protect our vital public and private installations around Singapore. The close co-operation seen in troop deployments to safeguard the Singapore Changi International Airport and petro-chemical hub at Jurong island are cases in point. The close civil-military coordination involved in securing the successful conclusion of high signature public events in Singapore (eg. *Asian Aerospace 2002 and Asia Security Conference* from 31 May-2 June 2002) and other key installations island-wide post 9-11 are also positive signs in the right direction. We have also tightened up border controls and stepped up cargo and immigration checks at all land, sea and air exit/entry points into our island republic. More work lies ahead and the various ministries and their agencies are separately spearheading reviews of our contingency and emergency plans under their respective purviews. Regular security exercises and mega-event security operations will continue to be jointly planned and executed to tap synergies and hone competencies.

- ## Enhanced Total Defence

It is clear that the fine line between external and internal defence has all but blurred, if not disappeared. Post 9-11 events have lent greater credence to the prudence and faith we had in instituting Total Defence for Singapore two decades ago. Total Defence has served well in conventional deterrence but it will now have to be enhanced further in the following areas to tackle the broader spectrum of threats:

  - National Psychological Resilience and Social Harmony. The key effect of terrorism is fear. It is therefore imperative to have national communication mechanisms in place to disseminate accurate public information and disabuse disinformation. This is vital in mitigating any climate of doom and gloom and to allow life to go on as normally as possible by cushioning the shocks of surprise attacks and weathering the storms of protracted adversity. The key objective will be to build up greater psychological and social resilience to weather the unpredictable storms of full spectrum conflict without descending into general hysteria or social paralysis. Another important aspect of terror to guard against, besides paranoia, is that of social suspicion and discord. Tensions can arise if misperceptions that certain segments of a society may be targeted for national security enforcement actions are not

promptly corrected and seen to be fair. Multiracial-religious states, especially one like Singapore, must tread a fine balance between maintaining security and managing sensitivities amongst the different groups. While there is a need to act firmly, states must be careful not to react over-defensively. The war against global terrorism is clearly not a religious or civilizational war, no matter how convenient and attractive the logic may seem to some. It is a war against transnational criminals who seek to tear the social fabric of nations by driving a bloody stake of terror and suspicion through its body politic. Ultimately, the real centre of gravity in the terrorism battle revolves around winning hearts and minds. Post 9-11, Singapore has taken a determined bottom-up approach to promote a deeper sense of social harmony. We have instituted new mechanisms like Inter-Racial Confidence Circles (IRCC) to enhance understanding and interaction amongst the various races and religious groups in Singapore. This is being done through grassroots outreach activities like inter-faith worship site tours, community club courses, working through TV media programmes and even breaking fast during the Month of Ramadan by the children and youths of the different religions. Schools are also another focus area where the common space of early interfaith and interracial interaction amongst young minds can be preserved, if not enlarged and strengthened. Tomorrow's social cohesion begins with good grounding of the younger generation today, and should never be assumed. It will always be work and dialogue-in-progress.

- Critical Infrastructure Assurance. In an era of Bio-Chemical and cyber threats, we are also paying greater attention to preserving our critical infrastructure in times of prolonged national duress. Vulnerability studies are being conducted to ascertain the extent of our strengths in sectors ranging from Transport, Communications, Water and Food supplies. The robustness of financial system from the broad spectrum of systemic infrastructure attacks spanning across physical, psychological and cyber realms will have to be looked into comprehensively.

• Developing New Capabilities & Leveraging on Technology

Another key focus of would be to seek out new capability developments and to do so by leveraging on technological advances where relevant. A National Security technology blueprint could be drawn up to define and develop *Big, Hairy Audacious Goals* (BHAG)[15] to thwart WMD terrorism. Take for example the goal that all joint security and civil defence forces must be prepared to conduct combined operations for extended periods of time in hazardous chemical and biological environments and to overcome this challenge through comprehensive protective measures on the ground, in the air and at sea. Of particular interest will be the development of better monitoring, surveillance and detection capabilities by exploiting emergent high technologies. To be sure, advances in deep-scanning, radiation-tolerant microelectronics, Artificial Intelligence and Biometric technologies have broadened the scope for future employment. Chemical and radiological spectral scanning technologies are also being actively explored to boost aviation and maritime check-point security. And for now, bio-sniffers remain the holy-grail of detection technologies. In fact, Singapore's public health authorities have recently announced plans to put aside a hefty $S100 million war-chest to build sophisticated laboratories and capabilities to detect quick-spreading infectious diseases and combat bio-terrorism. Weaponized bio-threats such as that posed by the potential return of a pandemic small-pox outbreak demands concerted syndromic vigilance by the international community *and* contingency vaccine stockpile planning by domestic public health authorities.

• Funding and Procurement

Another point well-mooted by many security analysts is that successful strategy must ultimately include the provision of meaningful guidance for resource allocation. The correct prioritisation of funding and procurement will lead to the development of the right capabilities to meet the real

threats. One of the key problems faced by many countries, like the US, is over the question of funding. When the respective national security project team studies are completed, we will be in a better position to refine the right strategies to pursue and identify/prioritise the key areas where funding commitment and smart procurement will give us the critical force-multiplier edge we so desire.

- ## Anti-Terror Legislative Mechanisms and Enforcement Powers

The nature of the new terrorism requires a bold legal approach to criminal prosecution. Blocking an actual attack, whether by disrupting the perpetrator's financial and logistical support or stopping attacks outright in a timely manner, requires more than intelligence and operational teeth. It requires legislative mechanisms to allow financial regulators to better monitor suspicious transactions, as well for enforcement agencies to effect preventive arrests to forestall attacks. In fact, Singapore has recently enacted a bill to counter money laundering and other means of financing terrorists. Not unlike the letter and spirit of the US's newly installed *Patriotic Act*, post-colonial countries like Malaysia and Singapore have inherited from the British, their respective *Internal Security Acts (ISA)* for prosecuting agents of terror, often even before they strike ie. arresting what the US calls 'enemy combatants'. Publicising successful pre-emptive security (CT 'sting') operations, like the recent Internal Security Department (ISD) arrests, may severely disrupt and disincline potential perpetrators and copy-cats from attempting terrorist attacks on Singapore. More importantly, they also underscore the continued relevance and functional utility of maintaining sharp legislative mechanisms like the ISA for preserving security. For all intents and purposes, the ISD is more than a domestic Intelligence Service. It is also a law enforcement agency with powers for crime pre-emption and prevention, and not merely*post facto* criminal investigation. In fact, in an effort to harmonise its intelligence function and enforcement powers, senior ISD Intelligence officers can now be given powers similar to that of police officers to allow them to exercise certain provisions under the ISA eg. for effecting arrests and detention. Following the normalisation, senior ISD intelligence officers can also be given police powers of investigation under the Criminal Procedure Code or other laws prescribed by the Home Minister. Officers will also be given immunity while carrying out a warrant similar to all police officers.[16]

- ## Diplomacy and Co-operation

At the broader international relations level, close bilateral and multilateral co-operation, like joint intelligence-sharing and enforcement operations are critical for effective global action against the new terrorism. No country can fight this war alone, if it hopes to win it decisively over the long-term. Security agencies with an external and internal orientation must find new ground to work with their foreign counter-parts. Enhanced interactions across the ministries and national agencies at the operational levels will minimise deviations and promote consistent policy alignments for diplomatic co-operation and domestic security synergy. The objective of our foreign policy will be to ensure that we stand on the right side of angels and secure the goodwill of friends and powers-that-be when we have to tackle the new threats, whether alone or as part of a wider regional/international coalition. On the latter point, new multilateral proposals like those floated at the recent inaugural Asia Security Conference (dubbed the "Shangri-La dialogue" after its Singapore hotel venue), calling for greater regional efforts in intensifying "backend cooperation" for CBRNE incident management and recovery exercises/operations may well be worth exploring, if sufficient common interest and political will can be found.[17] Already, Singapore has made bold inroads by being the first in Asia to sign-up onboard the US *Container Security Initiative*(CSI) to help pre-screen sea cargo headed for the US, thereby contributing in no small way to better help secure an important part of the global sea trade system. Singapore and Chinese law enforcement officials have also agreed to work together to exchange information to fight terrorism.[18] Sustained international collaboration and regional support will ultimately determine the degree of success in fighting the terrorism scourge together. It is a given that the foreign policies of small states, such as Singapore, are often dictated by complex national security interests and geopolitical imperatives.

Therefore, the diplomatic aims of Singapore's national security policy are necessarily conditioned by the threats we face and our inherent vulnerabilities - our physical size, geographical position, access to vital natural resources and dependence on freedom of international exchange and communications. They will continue to be safeguarded by pursuing the following principles:

- Securing peace and promoting prosperity in South East Asia and in the world as a whole;
- Respect for the independence and integrity of sovereign nations;
- Strengthening of the friendship and cohesion of ASEAN nations and like-minded partners both bilaterally and multilaterally;
- Opposition against aggressive activities of all types or interference against other nations;
- Free access by land, air and sea to all nations, based on the principles of free trade and enterprise; and
- Friendship with all nations respecting the sovereignty of the Republic of Singapore and the principles outlined above.

Conclusion: Networked Integration

The First War of the 21st century looks set to be a protracted one. Its disparate root causes will also not be resolved easily. Successful resolution may take generations, if ever. The difficult path ahead demands that we articulate clear and concerted national security strategies, backed-up by the polling of relevant national resources and key instruments of power. In prevailing over the new threats posed by what has been called an "organisation of organisations,"[19] in an era of "unknown uncertainties"[20], it is clear that we now need a *network to fight a network*[21] both on home soil or afar. It is perhaps a salutary testimony on the integration and steadfastness of Singapore's security and intelligence agencies when John Arquilla recently paid the following generous compliment: "Indeed, we have much to learn from *the skillful networking orchestrated by Singapore* late last year as it neutralized a major terror network node that was planning an ammonium nitrate truck-bombing campaign against American targets there."[22] But we cannot afford to rest on our laurels. Not when the threat is still out there and possibly still in here the second wave of Singapore arrests in August 2002 and similar ones in many countries around the world serve as a chilling reminder. [The latest message of mayhem from Bali has also "hit home" hard for many countries in the region.] In the main, the recent first anniversary commemoration should also remind us all that 9-11 was more than an indictment on the tragic failure of intelligence or imagination. More pointedly, it was a monumental failure in integration. The networked strategies and convergent structuring organisations outlined in this paper lay out the important transformational groundwork necessary for building a resilient National Security Architecture to safeguard the Singapore homeland. They also bring homeland security issues into sharp focus and accord them the high priority they urgently deserve. Convergent focus and coordinated action will be key. In an increasingly uncertain and polarised milieu, many countries can ill-afford to do any less. The home truth is that with many countries still reeling from the terror fallout of 9-11, we all badly need to put homeland security back on *terra firma*.

Endnotes

1 cited in Lydia Lim, 'National Security Secretariat Set-Up at MINDEF' in *The Straits Times*, (7 Jan 2002).

2 cited in 'Government Acts to Counter Terror Threats' in *The Straits Times*, (18 May 2002), p. H4.

3 See Oliver Morton, 'Divided We Stand' in *Wired Magazine*, (December 2001).

4 19 of the 21 are members of the JI network, while the others are linked to the Philippines-based Moro Islamic Liberation Front (MILF). See 'Another 21 Arrested Here Over Terrorism Plans' in *The Straits Times*, (17 Sep 2002), p.1.

5 Refers to a steady stress state over a prolonged period of crisis, whereby response demands may increase suddenly and then level off at a steady state indefinitely; until the next series of escalation or de-escalation activity.

6 Refers to a steady escalatory rise in response demands over a relatively short period of crisis, with rapid surge in response demands during anticipated high-tension periods. 7 Refers to systems that may fail because of attacks, but can recover quickly without losing too much of their systemic integrity and utility. See Charles, C. Mann, 'Homeland Insecurity' in *The Atlantic Monthly*, (Sep 2002), p. 82-102.

8 Cited in Kenneth Timmerman, 'Cracking The Afghan Network' in *Reader's Digest*, (May 2002), p. 112-28.

9 Thomas Friedman, 'Why Iraq Debate is Upside Down' in *The New York Times*, reproduced *in The Straits Times*, (19 Sep 2002), p. 17.

10 B Raman, 'Punishment Terrorism', (28 Mar 2002) available at*http://www.saag.org/papers5/paper431.html*

11 DPM and Defence Minister Tony Tan, cited in Robert Karniol, 'A Total Defence', in *Jane's Defence Weekly*, (4 Sep 2002), p. 25

12 *ibid*

13 See 'Task Force Ready To Swing Into Action On Security' in *The Straits Times*, (19 Sep 2002), p. 4.

14 See 'Government Acts to Counter Terror Threats' in *The Straits Times*, (18 May 2002), p. H4.

15 Exceptional organisations set challenging and often risky goals. BHAG is a concept advocated by James Collins and Jerry Porras, *Built to Last: Successful Habits of Visionary Companies*, (Harper, 1997); The concept has also been adopted by VP and Senior Scientist of *Sandia Labs*, Gerry Yonas, in Sandia's advanced technology R&D work; See also *Sandia LabNews*, Vol. 53, No. 8, (19 April 2002).

16 See 'Police Powers for Intelligence Officers' in *The Straits Times*, (25 May 02), p. H2.

17 See Ross Babbage, Recovering From Terror Attacks: A Proposal for Regional Cooperation, (July 2002), Australian Strategic Policy Institute Occasional Paper. Tangentially, business disaster recovery may be big business for Singapore with the setting up of a new professional certification body Disaster Recovery Institute (Asia) to raise the standards of business continuity planning in Singapore; See Simon Wilcox, 'Disaster Recovery May Be Singapore's Next Big Hit' in *The Straits Times*, (3 Sep 02), p. A16.

18 See Maria Siow, 'China & Singapore Agree to Cooperate to Fight Against Terror', in *Channel News Asia.Com*(3 Sep 2002).

19 Rohan Gunaratna's comments cited in 'Tapes Give Evidence of Al Qaeda's Global Reach', in *CNN.Com,* (23 August 2002).

20 DPM and Defence Minister Tony Tan, cited in Karniol, *Op Cit.*

21 See John Arquilla & David Ronfeldt, 'Fighting The Network War', in *Wired Magazine*, (Dec 2001); Thomas A. Stelwart, 'America's Secret Waapon', in *Business 2.0*, pp. 59-68; Ashton B. Carter, 'The Architecture of Government in the Face of Terrorism', in *International Security*, Vol. 26, No. 3 (Winter 2001/2), pp. 5-23; & Andrew Tan 'Government in The New Economy', in *Ethos*, Vol. 8 No. 2, (Singapore Civil Service College, 2002), pp. 9-15.

22 *Italics mine.* John Arquilla is Professor of Defense Analysis at the Naval Postgraduate School in Monterey, USA. See John Arquilla, 'It Takes a Network', in *The Los Angeles Times* (25 Aug 2002); also available at*http://www.rand.org/hot/op-eds/082502LAT.html* . See also John Arquilla & David Ronfeldt (eds.) *Networks and Netwars: The Future of Terror, Crime and Militancy*, (US, RAD, 2001).

COL Jimmy Tan is currently Commander, Air Defence Systems Division. He has been a branch head in HQ RSAF, a Squadron Commanding Officer, a Commander of an Air Force Brigade, a department head in the RSAF and Director, National Security Secretariat in the Defence Policy Group. He holds a BA (1st Class Honours) in Engineering Science from the University of Oxford (1984) and a Masters in Management Science from MIT. He attended the USAF Air Command and Staff College (Maxwell AFB) in 1990 and National War College in Washington D.C. in 1999.

MAJ Irvin Lim Fang Jau is an Assistant Director in the Defence Policy Group. A Principle Warfare Officer by training, he has served various operational tours in the Fleet. He holds a BA (First Class Honours) in Communications Studies from Murdoch University, an MBA from Leicester University and an MSc (Strategic Studies) from IDSS-NTU. He was the 1st prize winner of the 1998 CDF Essay Competition.

The SAF: From Training To Learning For Fighting Effectiveness

by LTC Richard Pereira

In the 1990s, organisational learning and knowledge management have become two important buzzwords in the domain of enhancing organisational effectiveness. While the importance of learning was never disputed nor made a contentious issue, it was predominantly in the last decade that many organisations have begun to take advantage of the revolution in information technology to reorganise themselves to increase organisational performance. At the heart of this reorganisation was the imperative by companies such as British Petroleum and Andersen Consulting to build a learning organisation - the kind that is not averse to learning, sharing ideas and expertise within and without the company while still staying fully committed to business unit performance.

The SAF too has to ride on this next new wave to increase organisational performance. At the heart of the SAF's mission is the imperative to win a quick and decisive battle. But how is quick and decisive to be defined? What key drivers cause a quick and decisive victory? Beyond the periodic acquisition of military hardware to expand its war-fighting capabilities, the SAF has also invested heavily in information technology since the 1980s to increase productivity and efficiency. However, where should the SAF draw its leverage and force multiplication capabilities from when such hardware and software lends itself to relatively unimpeded emulation?

A critical competitive advantage for the SAF in the new millenium will be its ability to learn faster than its potential competitors. A continuously and fast learning SAF will be able to translate quickly, hardware and software acquisitions into a relevant and potent war-fighting capability. Given the "young and lean SAF" policy and a fast-changing environment, this ability to learn fast and learn right becomes an organisational imperative. As the body of information and experience within the SAF continue to expand and deepen, so does the pressure to sieve out the relevant information and experience and translate them into the right knowledge for its subsequent use to improve our strategic war-fighting capabilities. A learning SAF must be able to translate what it has learnt directly into an effective war-fighting capability. Put another way, organisationally, the SAF should actively set out to learn that which would positively impact its operational effectiveness.

Conceptualisation of Learning

How should the SAF approach learning? In the early 1990s, British Petroleum (BP) became acutely cognizant that success in today's knowledge economy was highly dependent on the company's ability to harness a key source of competitive advantage - the ability to share among themselves the wealth of expertise, ideas and latent insights that "lie scattered across or deeply embedded in their organisation".[1] The other aspect of BP's philosophy was the fundamental realisation that learning need not necessarily be confined to the space within the organisation, but that really, the world was its oyster it meant that they must learn from anyone and anywhere so long as that learning will help BP create value for the company and shareholders. "You can learn from your own experience. You can learn from your contractors, suppliers, partners and customers. And you can learn from companies totally outside your business."[2] All are crucial for BP to be "the world's most successful oil company in the 1990s and beyond."[3]

As Andersen Consulting (AC) grew phenomenally from 1991, it had begun to become a victim of its own success and ambitions. The more vast and dispersed its operations became, the more complex knowledge management became. With over 50,000 employees, this was a daunting challenge. AC had to embark on a radical change to build a centralised, organisational learning capability, with a view to leverage on its vast knowledge and experience base, amassed after many years as a dominant player in management consultancy.

The SAF needs to conduct itself as a continuously evolving, learning organism. As it grows, it will continue to accumulate vast reservoirs of information and experience. The challenge is to translate the information and experience it possess and had accumulated into relevant knowledge, retain it, build upon it and even create new knowledge in an iterative manner; each time critically linking this process into the all-important war-fighting capabilities. Nancy Dixon defines it as "the intentional use of learning processes at the individual, group and system level to continuously transform the organisation in a direction that is increasingly satisfying to its stakeholders."[4] I therefore say that learning for the SAF should be strategic and geared predominantly toward enhancing fighting effectiveness to achieve a quick and decisive victory. This notion of learning-for-fighting effectiveness is distinctly different from a culture of learning that is geared toward personal learning, improving innovation and creativity, career advancements etc. The two concepts are not synonymous and the latter does not guarantee the former. Both are necessary but my contention is that the SAF has focussed more on personal mastery of fighting skills and it is therefore timely to shift this focus aggressively to embrace strategic learning for organisational-level or system-level fighting effectiveness.

Strategic Learning

Strategic learning for the SAF must be learning that is focussed on preparing the SAF for the vast spectrum of activities that the SAF will be called upon to undertake in the emerging dynamic environment. Preparation to meet the diverse challenges effectively is a key element of the strategic learning stance that is advocated here "preparation about learning relevant skills and capabilities, about learning to think in the right way, about developing emotional resilience, about learning to value your colleagues and so on."[5] To achieve these, organisationally, the SAF must be prepared to embrace change, in particular second-order change. Most organisations appear to focus on first-order change, that which is "within defined and acceptable parameters: it is about incremental change, which is often doing more of (or doing better than) what we have done in the past. Second-order change occurs when we move outside existing parameters and frameworks. It can mean even changing the way we change."[6]

Organisational Learning Imperatives

It is all too tempting to attempt a massive organisational change without first understanding several key factors that should drive such change. One of the critical imperatives is that even if learning does not take place, at the least, there should not be organisational forgetting. This is particularly critical to the SAF that espouses a lean and young posture. The need to be young implies a higher organisational turnover rate, particularly at the officer corps level. Organisational learning that is oriented at the individual level will suffer from this turnover behaviour. Linda Argotte refers to this as knowledge depreciation over time.[7] Related to this is the notion of organisational memory or organisational knowledge. If they are retained in "human portals", as predominantly tacit knowledge is today, then the organisational learning is impeded. Levitt and March argued that "the memory does not become organisational until it is captured in a repository that is not dependent on the vagaries of individual membership."[8] Here, I am referring particularly to knowledge that is embedded in an organisation's routines, standard operating procedures, processes, doctrines, technologies, equipment, culture, norms etc that which is crucial to the way we will fight. Another critical area is the need for the SAF to determine to what extent is knowledge embedded in the technologies that play such a crucial role in our war-fighting capabilities. The focus here is directed at pivotal areas such as electronic warfare and enhanced strike capabilities. Are we achieving the desired technology transfer? More importantly, are we structurally organised to facilitate technology transfer for operationalising our pivotal capabilities? Is our network of partners in the defence and defence-related industries similarly geared to harness, retain and build on the fruits of technology transfer?

Building A Learning Culture

At the heart of any significant organisational change is the need to change its culture. The SAF should embark on a massive, single-minded, deliberate effort to create a "learning-for-fighting effectiveness" culture. A key component of this change is the need for the top management to continuously articulate the purpose of this change and this is an important FIRST and necessary step in any transformation process.

The goal of this process is that the learning culture *is* the SAF and not a property that the SAF*has*.[9] The former perspective suggests that the culture is unique and mostly underlie everything that happens in the organisation while the latter idea suggests that culture is like the clothes we wear: it may be taken off when needed.[10] The former suggests a high degree of permanence while the latter may be more temporal. Cristina Zucchermaglio sums up neatly, saying, "learning is not a matter of transfer, but of construction. The learning process cannot be described by the metaphor of pouring something into an empty vessel: it is not true that information exists objectively and it is sufficient to simply transfer this into the learner's head. People are always active knowledge constructors and this is effected through interactions with the environment and the physical and social context in which they live Learning must be considered as a cultural development, a process of enculturation."[11]

The leadership must lead this strategic shift with command emphasis at every level and opportunity. Several channels may be exploited effectively to imbibe this culture of learning. As an example, a key component of BP's learning philosophy and culture was the top leadership's recognition that there was a propensity for mistakes during the learning process. The BP management was fully committed to supporting experimentation, which was believed to be integral to learning. "You've got to experiment. You've got to see what people actually do. You've got to see how the idea works. You've got to learn how to build something with a bit of track record which you can then apply more widely."[12] How close are we to this state of mind? The annual workplan is one critical avenue to initiate this change process toward creating a learning culture. This theme should permeate the services for several years to effect a discernible mindset change. The Army's decisive first step in this direction several years ago to actively construct such a culture is commendable but is also indicative of the massive time and effort required for its fruition. While the individual services attempt to chart their respective directions, the vision, mission and strategy must be articulated at the SAF level. A parallel effort at knowledge management must commence to invigorate the process of cultivating organisational learning.

Facilitating Knowledge Management

Several key issues that must be addressed when implementing knowledge management are elaborated later, not necessarily in order of salience. With more than three decades behind it, the SAF has accumulated vast amounts of experience, information and knowledge. The main challenge for the SAF is to determine what relevant knowledge should be extracted from its vast reservoir and how it should be managed in a sustainable way. More crucially, what important considerations underscore the implementation of a knowledge management mechanism?

- ### Information Overload

  With about 50,000 personnel in the SAF, it is easy to see why, eventually, there would be an information overload. In other words, the marginal value of additional data starts to decrease, culminating in negative returns. Edmund and Morris advised: "The machines we have invented to produce, manipulate and disseminate information generate information much faster than we can process it. It is apparent that an abundance of information, instead of better enabling a person to do their job, threatens to engulf and diminish his or her control over the situation. We can unwittingly allow information technology to become the driver instead of harnessing it as a tool to enhance rather than diminish our lives."[13] In fact, Edmunds and Morris go further to call this problem the information paradox "a surfeit of information and a paucity of relevant information", meaning that although there is "an abundance of information, if is often difficult to obtain useful and relevant information."[14]While technology allows us to manage the vast amounts of information, in the final analysis, the critical need is for value-added information.

- ### Definition of Knowledge

  The SAF should articulate the need to emphasise application of the relevant knowledge of high quality. But how is this to be defined? What is relevant knowledge of high quality? To what

resolution and fidelity can this knowledge be crafted? There is no doubt that knowledge acquired by the SAF over time will be a valuable asset. But there is a clear need to make a distinction between data, information and knowledge. The challenge is to create relevant knowledge. Wong and Radcliffe refer to tacit knowledge as the key driver. Tacit knowledge is not easily defined but is generally thought of as being "derived by experience, from learning by doing rather than from learning by theory. It is embodied in personal experience."[15] In a similar vein, the SAF must refer to the context in which the knowledge is created. Knowledge, devoid of the nuances of personal experience and context is at best termed information or what Wong and Radcliffe refer to as "explicit knowledge" .[16] They do acknowledge that tacit knowledge is difficult if not impossible to articulate or codify, but the importance of "explicating" embedded tacit knowledge has been acknowledged. It does therefore imply that much time and effort have to be expended to selectively acquire such knowledge. Too often, the difficulty of such an endeavour makes the acquisition of explicit knowledge the preferred path. Johannessen, Olaisen and Olsen caution that when enterprises invest in IT, "the focus will easily be on the part of the knowledge base that can be formalised, i.e. that can be easily be communicated to others as information. The tacit knowledge can then easily be de-emphasised since we can know more than we can tell."[17]In fact the authors emphasise the need to harness tacit knowledge to establish a sustainable edge (because it would be very difficult to be imitated) over our potential adversaries.[18]

- ## Validation of Knowledge

It is critical for knowledge to be validated so that "correct and relevant" knowledge is made available at every level in the SAF. Lee and Kwok have this to say about the organisational knowledge conversion process:

"The process of organisational knowledge management can be triggered by business problems or events. To solve them, an organisation's decision-makers can inquire about and search for related information, data or knowledge, sometimes seeking experts for ideas and suggestions. Human activities such as interpretation, understanding, analysing and reflecting will be very active during the knowledge management process. However, an individual's ideas or opinions can also be shared among organisational members until they are validated organisation-wide. Therefore, the decision-makers can try to justify their ideas, opinions, or information. After organisation members validate the new ideas or opinions into knowledge, the organisation can then apply the knowledge on its process or product."[19]

Quite clearly, information has to be validated before it is considered organisational knowledge. The SAF appears to have mastered this rather well at the tactical level. Doctrines, standard operating procedures, operating manuals are more frequently validated. However, to what extent is strategic level knowledge validated and institutionalised? Do we find access to strategic-level knowledge (or lessons) more cumbersome than tactical level know-how? Is knowledge equally transparent at all levels?

- ## Knowledge Transfer

A key precipitator of organisational learning is the ability for knowledge to be transferred across the vertical and lateral linkages of the organsiation.[20] However, security appears to be a major impediment to our realising this today. A consequence of this is the compartmentalisation of important knowledge at various levels within the SAF. The paradox between the need for knowledge sharing and security of knowledge need to be tackled much more vigorously and addressed as an organisational goal. This may become more challenging as the SAF increasingly incorporates more cutting-edge and secret-edge capabilities into her arsenal. However, as we move ever so closely toward an integrated fighting force, it becomes ever so critical for us all to be on the same knowledge wavelength to optimise our combat power.

- ## Time to Operationalise

  Anthony Byrd refers to the need to reduce "time-to-market" in order to develop a competitive advantage.[21] In other words, right knowledge, easier access and reduced reliance on inter-personal networks assure a higher probability of achieving quicker "time-to-market" solutions. George Stalk stated that time is as much a strategic weapon as productivity, quality and innovation.[22] Interpreted for the SAF, in the modern era, time has been "compressed" to the extent that speed of knowledge validation and operationalisation of critical capabilities now becomes a vital component. Friction and inertia in the form of overload, difficulty to access the right knowledge, etc have to be reduced to increase acceleration.

Putting It Together

I revisit the issue of second order change that was touched on at the start of this writing. The SAF must be prepared to embrace change that may be revolutionary, challenge the *status quo* notion of learning and demand more out of the organisational structure or its people. "An airline shifted their thinking from the idea that they were flying aircraft to the idea that they were flying people. So a technical/financial orientation switched to a marketing/customer care focus. In the process, the airline became a different kind of organisation with a different strategic direction. And the kind of learning needed to make this shift was totally different from anything they had experienced before."[23] Have we been focussing too much on being a peace-time SAF? Have we been focussing too much on being efficient at the expense of effectiveness? Should we re-orientate our minds toward being an ACTION-ready and effective SAF? Should we restructure for effectiveness that may mean being inefficient in peacetime? The asymmetry of the September 11 attacks is a stark reminder of how much we need to re-orientate current mindsets and to promote the kind of learning that will make the SAF more in tune with the diverse demands of the new age. My vision of an SAF War Centre (or SAF Learning Centre) that is the hub of research related to conflict and peace and the associated relevant learning requirements must be the next leap for the SAF. This high-powered centre should be empowered to dictate how the SAF should operate and the kind of learning capabilities that the SAF must build to support her operational imperatives in the future.[24]This centre will synergise learning and fighting-effectiveness to keep the SAF abreast of developments in the conflict resolution domain. Just as successful organisations rely on research and development as a cornerstone of their success, so should the SAF rely on a similar effort to keep it decisively relevant and effective.

Conclusion

I have attempted to elucidate a learning framework for the SAF in the sense that organisational learning in the SAF should relate directly to the way we intend to fight and to fight effectively. Several key factors must underlie the considerations that embrace cultivation of organisational learning. At the heart of this effort is the need to build a learning culture. For change to be deep, pervasive and open, this effort must be driven by the top leadership. In parallel, a mechanism must be put in place to facilitate knowledge management. The principal consideration in designing such a mechanism gravitate around a few critical issues such as information overload, knowledge definition, knowledge validation, knowledge transfer and so on. However the process is not complete without an organisational restructuring to drive and sustain organisational learning for superior readiness and performance.

Endnotes

1 Morten T. Hansen, Bolko von Oetinger, "Introducing T-Shaped Managers: Knowledge Management's Next Generation", *Harvard Business Review*, March 2001, p. 107.

2 Steven E. Prokesch, "Unleashing the Power of Learning: An Interview with British Petroleum's John Browne",*Harvard Business Review*, September-October 1997, p. 150. 3 Manfred F. R, Kets De Vries, Elizabeth Florent-Treacy, *The New Global Leaders*, San Francisco: Jossey-Bass Publishers, 1999, pp. 122.

4 Nancy Dixon, *The Organisational Learning Cycle: How We Can Learn Collectively*, London: McGraw-Hill Book Company, 1994, p. 5.

5 Ian Cunningham, *The Wisdom of Strategic Learning: The Self Managed Learning Solution*, London: McGraw-Hill Book Company, 1994, p. 27.

6 *Ibid*., p. 28-29.

7 Linda Argote, *Organisational Learning: Creating, Retaining and Transferring Knowledge*, Norwell, Massachusetts: Kluwer Academic Publishers, 1999, pp. 56-61.

8 *Ibid*., p. 72.

9 See Daniel Druckman, Jerome E. Singer and Harold van Cott, eds., Enhancing Organisational Performance, Washington D.C.: National Academy Press, 1997, p. 69.

10 *Ibid*., p. 71.

11 See Cristina Zucchermaglio, "Organisational and Cognitive Design of Learning Environment", in*Organisational Learning and Technological Change*, ed. Cristina Zucchermaglio, Sebastiano Bagnara, Susan U. Stucky, Germany: Springer, 1992, pp. 61-74.

12 *Ibid*., p. 160

13 Angela Edmunds, and Anne Morris, "The problem of information overload in business organisations: a review of the literature", *International Journal of Information Management* 20 (2000), p. 18.

14 *Ibid*., p. 22.

15 W. L. P. Wong, and D. F. Radcliffe, "The Tacit Nature of Design Knowledge", *Technology Analysis & Strategic Management*, Vol. 12. No. 4, 2000, p. 494.

16 *Ibid*., p. 495.

17 Jon-Arild Johannessen, Johan Olaisen, and Bjorn Olsen, "Mismanagement of tacit knowledge: the importance of tacit knowledge, the danger of information technology, and what to do about it", *International Journal of Information Management* 21 (2001) 3-20, p. 5.

18 *Ibid*., pp. 7-10.

19 Jae-Nam Lee, and Ron Chi-Wai Kwok, "A fuzz Group support system (GSS) framework for ogranisational knowledge acquisition", *International Journal of Information Management* 20 (2000), p. 387.

20 Linda Argote, *op. cit*., pp. 161-165.

21 Terry Anthony Byrd, "Information Technology, Core Competencies and Sustained Competitive Advantage",*Information Resources Management Journal*, April-June 2001, p. 32.

22 *Ibid*.

23 Cunningham, Ian, *op.cit*., p. 29.

24 See Arthur K. Yeung, David O. Ulrich, Stephen W. Nason and Mary Ann von Glinow, *Organisational Learning Capability: Generating and Generalising Ideas with Impact*, Oxford: Oxford University Press, 1999, pp. 121-141 for more elaboration on learning capabilities.

Bibliography

Argote, Linda, *Organisational Learning: Creating, Retaining and Transferring Knowledge*, Norwell, Massachusetts: Kluwer Academic Publishers, 1999.

Byrd, Terry Anthony, "Information Technology, Core Competencies and Sustained Competitive Advantage",*Information Resources Management Journal*, April-June 2001.

Cunningham, Ian, *The Wisdom of Strategic Learning: The Self Managed Learning Solution*, London: McGraw-Hill Book Company, 1994.

Dixon, Nancy, *The Organisational Learning Cycle: How We Can Learn Collectively*, London: McGraw-Hill Book Company, 1994

Druckman, Daniel, Singer, Jerome E., and van Cott, Harold, eds., Enhancing Organisational Performance, Washington D.C.: National Academy Press, 1997.

Edmunds, Angela, and Morris, Anne, "The problem of information overload in business organisations: a review of the literature", *International Journal of Information Management* 20 (2000).

Hansen, Morton T. and Oetinger, Bolko von, "Introducing T-Shaped Managers: Knowledge Management's Next Generation", *Harvard Business Review*, March 2001.

Jae-Nam Lee, and Ron Chi-Wai Kwok, "A fuzz Group support system (GSS) framework for ogranisational knowledge acquisition", *International Journal of Information Management* 20 (2000).

Jon-Arild Johannessen, Johan Olaisen, and Bjorn Olsen, "Mismanagement of tacit knowledge: the importance of tacit knowledge, the danger of information technology, and what to do about it", *International Journal of Information Management* 21 (2001) 3-20.

Manfred F. R, Kets De Vries, Elizabeth Florent-Treacy, *The New Global Leaders*, San Francisco: Jossey-Bass Publishers, 1999.

Prokesch, Steven E., "Unleashing the Power of Learning: An Interview with British Petroleum's John Browne",*Harvard Business Review*, September-October 1997.

W. L. P. Wong, and D. F. Radcliffe, "The Tacit Nature of Design Knowledge", *Technology Analysis & Strategic Management*, Vol. 12. No. 4, 2000.

Yeung, Arthur K., Ulrich, David O., Nason, Stephen W., and Von Glinow, Mary Ann, *Organisational Learning Capability: Generating and Generalising Ideas with Impact*, Oxford: Oxford University Press, 1999.

Zucchermaglio, Cristina, "Organisational and Cognitive Design of Learning Environment", in *Organisational Learning and Technological Change*, ed. Cristina Zucchermaglio, Sebastiano Bagnara, Susan U. Stucky, Germany: Springer, 1992.

LTC Richard Pereira is a pilot by vocation and is currently a Branch Head at HQ RSAF. He has held appointments as a flight commander and as a Squadron CO. LTC Pereira obtained an MSc (Strategic Studies) from IDSS, NTU and was the Tay Seow Huah Book Prize winner in 2001.

Riding The Crest Of RMA: Massive Systemic Shock Can We Do It?

by MAJ Roland Ng Kim Huat

The idea that rapidly evolving technologies will result in a profound change in the character of warfare in the coming decades, culminating in what has come to be known as a Revolution in Military Affairs (RMA) is generally accepted by all the military services in the world. Admiral Bill Owens, former US Vice Chairman of Joint Chiefs of Staff, advocated in his recent book, Lifting the Fog of War, that technology advancements in computers, sensors, satellites, wireless communications, and precision weapons formed the backbone to the current RMA.[1] According to him, the information-age technologies could potentially be the key to dissipate the hoary dictums about the fog and friction of war by fundamentally changing a military commander's ability to "see", to "tell", and to "act". The application of the new technologies into military system, coupled with the introduction of corresponding innovative operational concepts and organizational adaptation, will bring about a quantum leap in the capabilities of the military that rides its crest.

Although what will specifically characterize the possible end-states of this ongoing RMA is still evolving, it is commonly accepted that the core military imperatives have not changed. The military commander will still need to prepare for battle by collecting information to discern the salient points pertinent to his mission, and communicating the relevant subset effectively to his combat forces. The subordinate combat units will leverage on the information to identify and neutralise enemy centres of gravity, or target sets, in synchronised, simultaneous, and preferably precise operations.

What is new is that emerging information technologies now hold out a real prospect of allowing the commander to know more about the battlefield to have greater situational awareness of his own and enemy forces by orders of magnitude compared with past capabilities. He will also be able to receive, process and transmit information with unprecedented speed, and act on that information very rapidly with the use of precision force that will strike the enemy with devastating accuracy. In short, the tempo of operations will leap in quantum, creating revolutionary military leverages one great promise being able to induce massive systemic shock on the enemy's systems. As the SAF moves down the path of transformation to maintain its cutting edge in the new millennium, it is worthwhile for us to examine the relevance of this military leverage and the possible changes required for its realization.

Massive Systemic Shock

The technologies offered by the information revolution allow the military commander not simply to know more, but to know more faster and have the ability to act on that information very swiftly. Bill Owens used the notion of "System of Systems" to illustrate the interaction of separate technical applications, which together yield a powerful synergy that create the three conditions for combat victory: dominant battlespace knowledge, near-perfect mission assignment, and immediate/ complete battle assessment.[2]

Dominant battlespace know-ledge is a senior military commander's overall compre-hension of the enemy, his own forces, the battlefield terrain, and other factors that will influence the course of battle. The advance sensing and reporting techno-logies will be leveraged to provide the commander a real-time, three-dimensional picture of his battlefield with unprecedented fidelity, comprehension, and timeliness; by day and night, in any kind of weather, all the time. Platforms and the sensors associated with intelligence gathering, surveillance, reconnaissance (ISR), and reporting systems that provide better awareness of one's own forces will be maximised. Information technology will also be capitalised to provide accurate and timely information on weather conditions, landscape features that affect the manoeuvre and safety of the forces, and electromagnetic conditions such as enemy radio jamming.

Near-perfect mission assignment comes into play once the data is processed into information that is pertinent to the combat mission, and dispatched by the commander to his field units. The exchange of information between the headquarters and fighting units, and the transformation of raw intelligence data into relevant information, is made possible by high-volume, high-speed secure computer networks and communication channels linking all elements of the military force into a single entity. Subordinate combat commanders then use the available information to target and organise the battle to destroy the most important parts of the enemy force using the best-suited weapons available to carry out the mission.

Immediate/complete battle assessment enables the commander and his field units to assess immediately the success or failure of the strike so that they can carry out new attacks if necessary. With the advancements in information technology, powerful BDA (battle damage assessment) devices carried by conventional ground and sea platforms, manned aircraft and unmanned aerial vehicles, and space platforms will provide saturation coverage of the target areas in the shortest possible time in the day or at night under all weather conditions. Immediate and completes battle assessment complete the cycle by fully integrating intelligence, surveillance, and reconnaissance with the weapons and fighting force under a commander's supervision.

In tandem with the use of high mobility platforms and precision weapons, the information dominance enabled by the three conditions make possible the prospect of increasing the manoeuvre and strike tempo by orders of magnitude compared with past capabilities. This implies that future command cycles may be reduced from weeks or days down to hours or minutes. Instead of geographic massing of forces and fire, temporal massing for simultaneous attacks against an enemy's centres of gravity across the depth and breadth of the battlefield may be the dominant mode in future warfare. The combat forces will detect, identify and destroy a significant portion of an enemy's critical vulnerabilities faster than he can move, hide, or react. Taking it to the extreme, victory will be gained by inducing a massive systemic shock on the enemy's operating and control systems rather than a sequential attrition of the bulk of his forces.[3]

At the strategic plane, parallel strikes against critical targets across all levels of warfare from tactical units up through the national decision-making process can bring about the collapse of the enemy in a single blow. Even for sub-national terrorist groups using and operating from a given country but not necessarily sanctioned by the latter, the ability to take out all the elements from the top mastermind to the ground operative cells in a single covert, non-attributable surgical strike, such as lobbing precision munitions through the window of a warlord, may be a more attractive option with less fallout and repercussion. Indeed, Jeffrey Cooper suggested that a possible conceptual end state of the RMA might be the reduction of a protracted war to a "*coup de main* executed in a single main-force engagement".[4]

This is a compelling vision that is well suited to the SAF's defence strategy[5] and military principles of deterrence, as well as a swift and decisive victory. Achievement of this capability against the full range of our future enemies, from state-centric conventional forces to sub-national terrorist groups, will undoubtedly signify a new regime of warfare. At the very least, such high-tempo operations can swiftly eliminate our enemies' ability to project significant power that will threaten our forces and populace. At best, an enemy's belief in our ability to execute this type of operations will deter them from even contemplating aggression against us.

The technical breakthrough required to attain this capability is no small feat. For one, far more than the single sensor-to-shooter links common today, a system that could produce massive systemic shock will have to integrate large numbers of theatre sensors and weapons in real time a data fusion problem of tremendous proportions, and requiring breakthroughs in automatic target recognition technology and artificial intelligence. However, with terascale computing (three orders of magnitude beyond prevailing computing capabilities) looming at the horizon, it is not inconceivable that these technical difficulties will be resolved in the near future. The more difficult and crucial challenge is not the development and acquisition of the hardware but whether the SAF is structurally and functionally poised to leverage on this capability.

The Resources-Processes-Values (RPV) Framework

Clayton Christensen elucidated in his book, *The Innovator's Dilemma,* about the "failures of (good) companies to stay atop their industries when they confront certain types of market and technological change".[6] He then proposed a framework to help managers understand, when they are confronting necessary change, whether the organizations over which they preside are capable of tackling the challenges that lie ahead. His framework is equally useful for the SAF to understand the factors concerning how to bring about the military leverages enabled by information-age technologies. According to Clayton Christensen, three factors that affect what an organization can and cannot do are its resources, its processes, and its values (RPV).[7]

- ### Resources

  Resources in an organization are usually things or assets that can be hired or fired, bought or sold, depreciated or enhanced, and moved around easily. In a military organization, these are tangible assets such as our people, technology, defence budget and equipment. There are also less tangible resources such as national support for the military; information access through relations and interactions with external research agencies, academia, think tanks and foreign militaries; rapport with local and foreign defence industries; and level of integration with other agencies that have pivotal roles to play in the security of the nation.

  These are the inputs or ingredients that we put into the system to produce our capabilities. These are also the most instinctive areas where planners and decision-makers look for answers to assess whether our organization can successfully implement changes that confront us. There is no doubt that the presence of abundant resources will increase our chances of coping with changes. The SAF has thus far maximised its resources to propel its growth from a rudimentary force of two infantry battalions at its inception to a "most impressive military force in contemporary Southeast Asia"[8] that stands out within the region for the absolute and relative size of its defence budget, the technological sophistication of its forces and its model of military mobilization.

  With the defence budget pegged at 6% of our GDP, the SAF has benefited from the prosperity of the country with defence expenditure increasing by leaps and bounds from US$12 million in 1967 to more than US$4 billion annually in the late 1990s.[9] This has provided the means to finance the rapid but well-planned capital acquisition and technological capability build-up. To compensate for natural constraints of lack of strategic depth and a small population base, technology has been aggressively exploited as the force multiplier. The equipment of the SAF is continually enhanced, both through procurement of new systems from foreign suppliers and through upgrading existing hardware locally by a "military-industrial complex" that capitalises on the close triangular relationship strategically nurtured between the SAF, DSTA and ST companies. The determination of the SAF to develop defence R&D has culminated in the corporatisation of DSO National Laboratories, establishment of Temasek Laboratories and Temasek Defence System Institute (TDSI), and more extensive and in-depth collaboration with reputable military and civilian R&D establishments of advanced countries. As Tim Huxley observed, Singapore's wartime mobilization of human and other resources is "on a scale probably matched only in Israel, the European neutral states and the remaining Asian communist states".[10] The total mobilised personnel strength of 350,000, a great bulk comprising NSFs and NSmen, has high educational levels and is increasingly IT-savvy. This facilitates the extensive introduction of complex and technologically advanced information-age systems.

  Singapore is clearly prepared to invest in defence. The SAF has the means to acquire the information-age hardware, the know-how to integrate them and the personnel to operate them. Drawing lessons from the Gulf War and the Kosovo conflict, the SAF has already invested more resources to acquire and develop advance systems that could provide comprehensive battlefield awareness, precision strike and dominating mobility the three components required for high tempo operations.

However, there will be a limit to the amount of national resources that can be deployed for national security. The current recession should serve as a reminder that high economic growth and hence sufficient defence budget cannot be taken for granted. Even without the recent economic downturn, there are views that the present level of investment may be as much as the nation can afford. Fortunately, resource analysis does not give the final verdict on what sorts of innovations an organization is capable of assimilating to scale new heights. Even two organizations with identical sets of resources will have different abilities to embrace technological breakthroughs and innovations. This is because the capabilities to transform the resources to winning solutions and products reside in the organization's processes and values.

- ## Processes

Processes[11] refer to the patterns of interaction, coordination, communication, and decision-making that employees in an organization use to transform resources into product and services of greater worth. They are established so that staffs perform tasks in a consistent way, time after time. There are formal processes that are explicitly defined and documented. These are more visible. There are also informal processes routines or ways of working that evolve over time. These are less visible. In a military organization, there are processes that govern force development, equipment procurement, technology research, human resource management, and budget planning. At the operational and tactical level, doctrines and tactics are also processes that serve as guides to solve battlefield problems. Regardless, they are defined or evolve *de facto* to address specific tasks. If used to execute tasks for which they were designed, they are likely to perform efficiently. But, when used to tackle very different tasks, they are likely to seem slow, bureaucratic and inefficient.

Since its inception, the SAF has developed efficient and effective processes that enable it to progress to its current state. However, it has not fallen into the trap of self-complacency and allowed its processes to ossify. Contrary to the stereotype impression of a military organization being bureaucratic and hence resistant to changes, the SAF has been constantly at the forefront to "deconstruct" and initiate changes to prepare itself for the future. This was evident from the implementation of the innovative Saver and New Partnership scheme to tackle its personnel recruitment and retention concerns. Another illustrative example was the restructuring of DTG resulting in the corporatisation of DSO to become DSO National Laboratories and establishment of DSTA as a statutory board.

To make the transformation to an information-age military organization that is capable of executing high-tempo warfare, the SAF will again need to "deconstruct". The processes to adopt are still evolving and will require further research. However, finding answers to three critical questions will certainly improve the prospect of developing processes that are apt at inducing massive systemic shock on the enemy's systems.[12]

The first question to ask is what needs to be known about the enemy. The goal of inflicting a massive systemic shock is to knock the enemy into a state of concussion, thereby paralysing his ability to act and react, and collapsing his will to fight. This requires rapid identification and destruction of that set of critical vulnerabilities upon which the enemy draws its strength. In the linear approach of the past, cues could be taken from indicators as the battle unfolds, to discern the critical vulnerabilities. These vulnerabilities could then be destroyed sequentially to bring about the defeat of the enemy. Now, in order to achieve a non-linear, systemic effect, there may be a need to find out all the critical vulnerabilities in a substantially compressed time, sometimes even before the first shot is fired. Moreover, each of the enemy's vulnerabilities may involve target sets that vary greatly in both numbers and types, and which change constantly over time. The targeting of these vulnerabilities will also produce different effects on the psyche of the enemy soldiers, ranging from confusion to a sense of hopelessness in continuing the fight. This requires not only more understanding about how the enemy system operates, but also how the mind of the individual enemy soldier will react to our actions.

The processes to deduce solutions for such complex questions will require the aid of advanced computer modelling and simulation to provide greater insight, though the effectiveness of this analytical effort can only be as good as the intelligence that is available for examination. To this end, efforts to strengthen processes and capabilities in intelligence gathering and analysis will have to be stepped up, especially in the wake of an increased terrorist threat.

The second area that needs to be re-examined is the SAF's action cycle, focusing on how fast it needs to know and act. Sun Tzu's observations in 500 B.C. that "just as water retains no constant shape, so in warfare there are no constant conditions"[13] is still a truism today. At different times, the enemy will have different weaknesses. As a result, the critical target sets of the enemy's prevailing vulnerabilities are ephemeral. Revolutionary leverage emanates not just from identifying them, but from doing so very rapidly faster than they can move, hide, or adjust. This may warrant a near-real time OODA cycle with target identification-to-destruction in the order of hours if not minutes. For a large, highly complex adversary, the seamless integration of the ability to "see", to "tell" and to "act" will be required for near simultaneous identification and targeting of thousands of critical vulnerabilities.

The ability to conduct such operations may require a revolutionary change to the SAF's existing command and control (C2) structure and processes. The demand for near real-time simultaneity in all arenas of operations warrants a need to ruminate upon the benefits of a single joint command set-up *vis-à-vis* separate campaign HQs model in order to cut down time-delay in battle co-ordination. The need for speed may force today's hierarchical command structure to a flatter and more network-oriented model that will facilitate diverse and dispersed actors to operate together rapidly across greater distance than before.

Beyond the issues of C2, the most critical drag on high-tempo system performance is actually the cognitive limit of the human mind, the rate at which an individual can assimilate information and act. An information-intensive battlespace may require humans to be largely removed from the lower command loop, with analysis and decision-making extensively replaced by artificial intelligence and automated systems instead of time-consuming human deliberation.

Last but not least, the SAF needs to decide how much it is willing to invest in the new capability. The fact that the SAF is at the point of transforming into an information-age military will not be lost to its adversaries. Even if the adversaries may not be able to match the SAF in terms of resources to build up their systems, they can resort to asymmetric solutions. The acquisition of target data and precision-guided munitions will continue to be big-ticket items even with the advent of increasingly powerful and cheaper microprocessors. A clever enemy can always devise unsophisticated and inexpensive counter-targeting techniques that will keep the SAF on the wrong side of the exchange ratio, rendering it much less expensive for him to deny timely information than for the SAF to gather it. Whether the SAF can achieve a revolutionary effect with information before a clever adversary makes that information too costly may be the most critical challenge in its future processes.

The alternative option of expending large numbers of smart munitions to overcome ambiguity in targeting data is not viable as this may give the SAF a military victory at the expense of imposing a considerable burden on our economy. The chances of greater collateral damage will also increase. This may prompt the enemy to resort to a war of attrition and general destruction. Taking this consideration one step further, protection and strike are actually two sides of the same coin. As the SAF builds up the capabilities to conduct precision warfare, resources must also be allocated to protect its critical vulnerabilities to protect them from the enemy's exploitation. There is therefore a need for processes that are cost-effective in "counter-counter-targeting", and well balanced between strike and protection. In the course of inducing massive systemic shock on the enemy's systems, the nation must not be rendered vulnerable both economically and militarily.

Summing up, the search for answers to these questions is not the destination but the start of a journey. The true value lies not in the answers themselves but the discovery of more questions. The

right questions can help the SAF take a hard look at its current processes and evaluate if they are apt at leveraging the disruptive technologies. The right decisions can then be taken to either revise its current processes or develop new processes that enable it to acquire new capabilities. These decisions nevertheless will be linked to the organizational values that shape the SAF's strategic direction and "business model".

- ## Values

Within the Resources-Processes-Values framework, values have a broader meaning than its usual ethical connotations. Clayton Christensen defined values[14] as the criteria by which decisions about priorities are made. Values will allow personnel throughout the organization to make independent decisions about priorities that are consistent with its strategic direction and business model. According to Clayton Christensen, when assessing whether an organization can address disruptive change successfully, an important area that should be focused on is the value that dictates what the organization judges to be acceptable gross margins.[15] Adapting his theory to a military organization, this can be translated to the basis by which the military judges what is favourable combat effectiveness.

In general, the industrial age military measures combat effectiveness by numbers number of enemy soldiers that it can subdue or number of platforms that it is able to neutralise by its actions. As long as the organization is fixated with numbers, missions will be planned to achieve favourable force exchange ratio, and emphasis will be placed on hard kill of physical entities. A simple rule of thumb summarises it all: That cannot be counted, cannot be used as indicators for success. This inevitably will lead to attrition warfare that is an antithesis to a key aspect of the current RMA the discrete application of force thereby achieving economy by substituting quality for quantity.

For an information-age military that seeks to induce massive systemic shock on the enemy's systems, combat effectiveness may need to be viewed from a different perspective. Instead of doing head count, a more suitable measure could be to gauge combat effectiveness in terms of effects on the enemy systems. This does not mean that physical destruction of the enemy forces is no longer necessary. However, it advocates a shift in emphasis from platform-centric overmatch to system-centric overmatch. The measure of effectiveness is no longer about whether one of our tanks can match two or three of the enemy's tanks. Rather, the focus is on "shocking" the enemy system by dislocating it geographically, temporally and psychologically through integrated application of our assets as a system. The synergistic and force multiplying effect may well allow the achievement of Sun Tzu's ideal of overthrowing "kingdom without lengthy operations in the field".[16]

A value change will affect the standard by which priorities are set to judge whether an order is attractive or unattractive, whether a task is more important or less important, whether an idea for a new way of fighting is appealing or marginal. At the ground level, they will shape on-the-spot, day-to-day tactical decisions. At the management level, they will influence the decisions to invest, or not, in new equipment, technology, and processes. Just as the fruits of the RMA labour are not yet crystal clear, the debates on "RMA-correct" values are still on-going. Regardless, for the SAF to be able to induce massive systemic shock on the enemy's systems, a re-look at its fundamental values is necessary.

Conclusion

Deputy Prime Minister and Defence Minister, Dr Tony Tan, when speaking at the graduation ceremony of the Second Command and

Staff Course for operationally-ready national service (NS) officers on 7 Nov, said that "Any would-be perpetrator must know that the SAF is alert and prepared for contingencies. Those who seek to inflict harm on Singapore should be left in no doubt that we have the means to take action against them."[17] To this end, the SAF must stay relevant and maintain its cutting edge by riding the crest of the current RMA rather than

follow its wake. The ability to induce massive systemic shock on the enemy systems is an interesting RMA military leverage that we should seriously explore.

End Notes

1 Admiral Bill Owens, pp98 -100.

2 Admiral Bill Owens, pp100 -103.

3 James R. Fitzsimonds, "The Coming Military Revolution: Opportunities and Risks", *Parameters*, Summer 1995, p31.

4 Jeffrey Cooper, "Another View of the Revolution in Military Affairs", US Army War College, Strategic Studies Institute, 15 July 1994, p30.

5 J.N. Mak, ASEAN Defence Reorientation 1975 1992: The Dynamics of Modernization and Structural Chang, (Canberra: Strategic and Defence Studies Centre, Australia National University, 1993), p162.

6 Clayton M. Christensen was referring not about the failure of any company, but of *good* companies, those that many managers have admired and tried to emulate, the companies known for their abilities to innovate and execute.

7 Clayton M. Christensen, pp162-166.

8 Tim Huxley, p249.

9 Tim Huxley, p27

10 Tim Huxley, p.xx.

11 Clayton M. Christensen and Michael Overdorf, "Meeting the Challenge of Disruptive Challenge", *Harvard Business Review*, March April 2000, p68.

12 James R. Fitzsimonds, "The Coming Military Revolution: Opportunities and Risks", *Parameters*, Summer 1995, p32-33.

13 Sun Tzu, p36.

14 Clayton M. Christensen, *The Innovator's Dilemma When New Technologies Cause Great Firms to Fail*(HarperCollins Publishers, 2000), pp164.

15 Clayton M. Christensen and Michael Overdorf, "Meeting the Challenge of Disruptive Challenge", *Harvard Business Review*, March April 2000, p69.

16 Sun Tzu, *The Art of War* translated by Lionel Giles, Stackpole Books, 1985, p27.

17 Bites of the Week (10 - 16 Nov 2001), "Intelligence Networks a Vital Defence: DPM", SG News Web Site.

Bibliography

Admiral Bill Owens, *Lifting the Fog of War* (New York: Farrar, Straus and Giroux, 2000).

Bites of the Week (10-16 Nov 2001), "Intelligence Networks a Vital Defence: DPM", SG News Web Site.

Clayton M. Christensen, "The Innovator's Dilemma When New Technologies Cause Great Firms to Fail", (Harper Collins Publishers, 2000).

Clayton M. Christensen and Michael Overdorf, "Meeting the Challenge of Disruptive Challenge*", Harvard Business Review*.

James R. Fitzsimonds, "The Coming Military Revolution: Opportunities and Risks", *Parameters*, Summer 1995.

Jeffrey Cooper, "Another View of the Revolution in Military Affairs", US Army War College, Strategic Studies Institute.

J.N. Mak, ASEAN Defence Reorientation 1975 1992: The Dynamics of Modernization and Structural Chang, (Canberra: Strategic and Defence Studies Centre, Australia National University, 1993).

Sun Tzu, *The Art of War* translated by Lionel Giles, (London: Stackpole Books, 1985).

Tim Huxley, *Defending the Lion City The Armed Forces of Singapore*, (St Leonards, NSW: Allen & Unwin, 2000).

MAJ Roland Ng Kian Huat is a Weapons System Officer (ADA) by training and is currently a Branch Head at MINDEF. Previously he held the appointments of Branch Head at HQ ADSD and Squadron PC. He graduated with a Masters of Engineering from University College London.

A Culture For Transformational Change - Strategies For The Singapore Armed Forces

by MAJ Seet Pi Shen

"In military affairs, especially in contemporary war, one cannot stand in one place; to remain, in military affairs, means to fall behind; and those who fall behind, as is well known, are killed."

Joseph Stalin[1]

Stalin's success in motivating Russians to adapt and fight under extremely trying conditions and to turn a seemingly hopeless situation against the Germans into victory in World War II underlies the importance for armed forces to survive and even thrive in times of continuous change, bordering on chaos. Organisations today are facing a change more extensive and more fundamental in its transforming quality since the 'modern' industrial system took shape in the early 1900s.[2] *Even without world wars, with rapid social and technological changes, shrinking defence budgets, the drive towards information age warfare, increasing involvement in peacekeeping operations and operations in asymmetric theatres, armed forces must continue to renew their roles to remain relevant.*

"Organisational culture can hold an organisation hostage to its past."[3] *The military, an organisation steeped in history and tradition, has always been a likely hostage candidate. Past glories have often led generals to prepare their armies to fight the previous war, not the battles of the future. The decisive defeat of those who have not succeeded in overcoming this tyranny of success has conveyed a clear message to the military leaders of today. That message is that change must be embraced in all its forms. To successfully achieve this, a military culture that is enthusiastic about change must be created.*

The aim of this essay is to develop strategies for the creation of a Singapore Armed Forces (SAF) military culture that embraces positive transformational change in an era of unprecedented uncertainty. It will briefly highlight what transformational change is, the need for the SAF to embrace it and why military culture is an important determinant. Following that, five strategies will bedeveloped to assist in creating such a culture. Firstly, there is a need to anchor a change of culture on values and vision. Secondly, we will need to breed creativity, which ties in thirdly, with the need to take risks and accept mistakes. Fourthly, training can facilitate cultural change. And finally, the SAF needs effective leaders to lead the change and working hard at communicating, grooming and caring for our people.

This essay will explore best practices from the commercial and military sectors and from history to develop some specific strategies that are relevant and applicable to the SAF of the 21st century.

Why Transformational Change?

Today, the world has changed significantly and is expected to continue at ever-increasing *volumes*,*momentum* and *complexities*.[4] The old paradigm believed in equilibrium, that things could be stable and efficient. The new paradigm replaces equilibrium with that of a chaotic world.[5] Many organisations, including armed forces, have adopted incremental approaches to adapting to chaos but have trapped themselves in an organisational treadmill, blinding themselves to a new perspective on tackling new issues and problems.[6] Organisations need to undergo a paradigm shift from being comfortable in equilibrium to being comfortable with continuous change. need to give way to cultural values of change and problem solving, electronic technologies, mental tasks, horizontal hierarchies, and dispersed power and control.[7]

Like businesses that want to remain competitive, the military will need to transform and adopt a culture that is highly adaptable and values change. Otherwise it will always have to play catch-up and thus be ill-prepared for the next major operation or war.

Military Culture Strengths and Obstacles to Transformational Change

Given the need for transformational change in military forces, what role does military culture have to play? An organisation's culture can be thought of as its collective "personality" that defines and constrains its behaviour very strongly. Transformation means changing some of those ingrained behaviours and convincing people that the new ideas are substantive, not merely the latest fad.[8]

Cultural barriers are often the most potent barriers to organisational change and military forces are no exception. Patton observed that armed forces "tend to consider the most recent past war as the last word, the sealed future pattern of all contests we realise, none better, that in the last war it was necessary to make many improvisations and to ply our trade with ill-assorted tools."[9]Professor Don Snider, from West Point, argues that this is largely due to the military "control culture" as *"its central elements derive from an attempt to deal with* (and if possible overcome) the uncertainty of war, to impose some pattern on war, to control war's outcome, and to invest war with meaning and significance."[10] Compounding cultural obstacles include a combat-masculine-warrior "enculturation", exclusive policies, separatist attitudes, hostile interactions and strong sub-cultures, like the individual Services who guard their domains stubbornly.[11] The results are "bureaucratised" forces with authoritarian leaders with poor internal communications, ignoring possibilities and creativity. [12]

The challenge is for SAF leaders to retain the fundamental aspects of military culture which enable it to fight and win, whilst fostering cultural characteristics which are more likely to embrace transformational change. The ability of the military's culture to adapt to the new paradigm could well make it the most important factor in preparing military organisations for the next war.[13] The challenge will be to build on the supportive while overcoming the resistant strands of military culture.

Transformational Change A Model for the SAF

Using a systems approach to the proposed strategies, the diagram below briefly illustrates a model that will give the SAF the strength to withstand the rigours of change. Each building block plays a key role, though once constructed, the framework is self-supporting and works as an integrated system. The framework shows culture as the foundation on which to build the new organisation. A shared vision sits at the top providing a clear, long-term focus in meeting future challenges while the values provide the firm foundation. The building blocks that form the super-structure of the organisation are made up of another three strategies.Firstly, fostering a creative climate that harnesses everyone's creative potential in developing innovative solutions. Secondly, flexibility must complement creativity, encouraging debate and risk-taking as well as tolerating mistakes and disseminating lessons. Thirdly, training people psychologically to better cope with changes. Finally, leadership, shown as the construction crane, acts as the builder that bonds everything together and keeps the organisation focused on the vision. All the components are interdependent and linked to provide strength and durability.

Strategy One Anchor Change on Core Values and a Shared Vision

Transformational change often brings about significant organisational upheaval. To hold together various subcultures and provide a secure anchor in the turmoil, thereby alleviating fear without raising resistance to change, military leaders must reinforce core values and develop a shared vision to mobilise and give meaning to people in crisis periods.[14]

A shared vision is a way of expressing deeply held values, essential in developing a common purpose and commitment, and it should energise the organisation in its acceptance of positive, transformational

change.[15] To be successful, it needs to give employees the three elements of "direction, discovery and destiny".[16] Avis' "We Try Harder" vision turned the company around with employees at every level responding to be better than "number two" by working harder and being more flexible than before.[17] The SAF has developed a set of seven Core Values in 1997[18] and these should be reviewed frequently as militaries undergoing change have also developed new shared visions to meet the future.

If values form the foundation of the military culture, then vision provides the direction. Vision is "an imagined possibility, stretching from today's capability, providingan intellectual bridge from today to tomorrow, and forming the basis for looking ahead, not reaffirming the past or *status quo*."[19]

Lack of clear vision undermines military innovation as it diffuses the creative effort. Due to a lack of vision, the British military in the inter-war years suffered from an innovation handicap and was ultimately ill-prepared for all eventualities. The absence of priorities also resulted in heightened inter-service rivalry and a wait-and-see approach. Conversely, clear visions in Japan and the United States enabled their militaries to innovate with clearer purpose - the development of the aircraft carrier being a prime example. [20]

The SAF must continually renew its vision for the future. An example is the Army's vision "*Army 21: The Decisive Force*" that was developed to bond the organisation to meet up to any challenge in the next millennium.[21] This is a good start but what is needed is that the values need to move beyond books and posters and that people in the SAF take on these shared core values and vision. This will engender trust that underlies the relationships among organisation members especially in tumultuous times. Similarly, keeping the shared vision relevant will provide focus in meeting the challenges of the future. Together, they form the foundation on which specific strategies for transformational change in any organisation is built.

Strategy Two Foster Creativity by Creating an Ambidextrous Organisation

Military forces are often sceptical of peacetime creative ideas and only resort to battlefield innovation in wartime. Hence, besides good leadership, the supporting staff should develop solutions that are innovative and responsive to future challenges. Today's business paradox is to "keep everything running and at the same time change everything."[22] This dilemma is of particular relevance to the military as it must maintain its readiness levels but at the same time implement change.

To overcome this paradox, the SAF can create an ambidextrous organisation, one that contains two separate change cultures in parallel, which are linked by a strong common vision.[23] The main body of the organisation remains functioning along traditional lines, carrying out daily operations and engaging in incremental change to improve existing process. A small secondary sub-culture is also created which is specifically intended to experiment, develop, test and introduce transformational change to the organisation. The advantage of an ambidextrous organisation is that it minimises the turmoil surrounding the introduction of change. In the case of the military, it also circumvents some of the challenges presented by the more *laissez faire* aspects of a truly innovative sub-culture clashing with the strict military command and control hierarchy.

One approach is to create a separate creative sub- culture in the organisation, putting people in teams "psychological safe havens"[24] to brainstorm and develop innovative solutions. These teams, insulated from external interference, will be able to "challenge mental models". [25] The US Army in the early 1990s created a separate sub-culture called the Louisiana Manoeuvres Task Force, named after the very successful change programme run by General George Marshall during the lead up to the United States entry, to World War II. The name signalled to the US Army the intention to introduce major change and also created a positive image by association with a previous successful transformational change. While not running specific projects, the Task Force circumvented bureaucracy, crossed horizontal boundaries, facilitated technological breakthroughs and fast tracked systems development. As a result, the Task Force was able "to introduce change much more rapidly across the Army than would otherwise have been possible." [26]

A commercial example is Microsoft's new-venture teams that give free reign to each member's creativity because their separate facilities and location free them from organisational rules and procedures. Such

teams are typically small and loosely structured and include a mix of experience and personalities. They target people with "bandwidth", a breadth of interest, and throw them together in mixed teams of "nerds" and sensitive designers. They are given clear goals and the resources they require. The resulting creative tension produces unique and innovative results.[27]

The SAF has already adopted a similar system that specially selects junior officers to work in project teams, addressing critical issues facing the SAF in the future.[28] Besides being different, the solutions adopted are more readily implemented as the future SAF leaders feel they are stakeholders to the plans. The challenge today for the SAF is to expand the intent of its project teams to include those further down the hierarchy. If all the people buy-in to the organisational goals, it will be much easier to drive changes.

A possible model is that of the US Marine Corps. At the soldier level, the strictures of discipline, orders and drills easily constrict creativity. However, the US Marine Corps' Marine Corps Combat Development Command (MCCDC) has shown that in the rapidly changing future battlefields, soldiers who have high-quality, "out-of-the-box" thinking will operate better.[29] The MCCDC has adopted the slogan "*Every Marine an Innovator*" and intends that all Marines participate in the transformation process from operational concept to operational capability. To facilitate this, pocket-sized booklets have been distributed to all Marines highlighting the latest draft concepts. Marines are encouraged to write-in or visit special web-sites and join in threaded discussion groups. The intent is to tap the creative potential of individual Marines to come out with better ideas, ones that senior people may have overlooked.

The challenge today is not to be the most creative boss or to have the most creative HQ staff. The challenge is to have the most creative organisation, limited only by the collective imagination of all of its constituents.

Strategy Three Taking Risks, Encouraging Debate, Allowing Mistakes and Learning from Them

Together with developing creative solutions, military leaders should not be too quick to dismiss or ignore new military ideas and concepts. The military's resistance to creativity is evident in buzzwords like "Standard Operating Procedures" (SOPs), "doctrinal templates" and "zero defects".[30] There are risks in seeking improvements and experimentation and mistakes will be made. However, if the senior leadership has bought into the importance of propagating the climate of creativity, mistakes will be tolerated and will encourage people to try harder in developing their ideas. This will make people believe they can change their environment, a necessary condition for a learning culture. [31]

Recognising people who take risks is a valuable strategy that conveys a clear message to others. Hershey Foods introduced the *"Exalted Order of the Extended Neck*" to recognise and reward employees who displayed a determination to take on risk.[32] When mistakes do occur they should be accepted positively by management if they are based on analysis, fosters learning and are modest in impact.

A key consideration in a military environment is that contrary opinions should not be taken as disloyalty. General Walter Ulmer observed that "the absolute authority essential in battle can be a spawning ground for abuse of power [in peace]."[33] General Colin Powell described a possible solution that lay behind the success of Operation Desert Storm, "When we are debating an issue, loyalty means giving me your honest opinion, whether you think I'll like it or not. Disagreement, at this stage, stimulates me. But once a decision has been made, the debate ends. From that point on, loyalty means executing the decision as if it were your own."[34] A military learning organisation must encourage open debate and reward intellectual development in order to be innovative.

The French-German contrast in the 1930s illustrates the pitfalls of an anti-debate, risk-averse approach. The French Commanding General Gamelin actively discouraged dissenting opinions and insisted on approving all articles, lectures and books written by serving officers. One French General noted that "everyone got the message, and a profound silence reigned until the awakening of 1940."[35] In contrast, the German Commanding General, Hans von Seeckt developed a cultural ethos that emphasised intellectual as well as operational and tactical excellence.[36] He placed a high value on open debate and analysis of changes in

doctrine, tactics and technology, creating a climate ideally suited to innovation. The German *Kriegsakademie* (Staff College) generated an officer corps capable of innovating in peacetime more effectively and realistically than its opponents.

Learning from this, we must be prepared to accept mistakes, associated with experimentation, in peacetime rather than wartime. The US Army's After-Action Review (AAR) is a method in which others in the organisation can learn from one's mistakes without necessarily going through the entire painful process. Its value to the US Army has spread to activities other than training and its success is dependent on the ability of leadership to be tolerant of mistakes in the learning and experimentation process and for these lessons to be shared readily.[37]

If an organisation is expected to become a culture that embraces transformational change, then its leadership must sell these clear and simple messages about acceptable behaviour.

Learning from mistakes is an important component in developing a learning culture that will form the backbone of the "Learning Organisation", one that "is continually expanding its capacity to create its future."[38]

Strategy Four Training For Change And Chaos

Time compression, not speed, defines the information age.[39] Chaos and friction in war will be sustained not by lack of information, but by too much information and too little time for analysis. Indecision and reduced tempo are the dangers. The SAF must develop intuitive commanders who thrive in a time-compressed environment in peace or war.

Training of commanders must promote decision and calmness in chaos. Disorder should be practised in day-to-day activitives and promoted in culture. This conflicts with traditional military bureaucratic values and technocratic discipline that seek to impose routine, order and logic. Because chaos threatens peacetime efficiency and increases risk, it is generally avoided in the militaries.

The SAF must maximise opportunities for future commanders to gain operational experience in its widest sense. As Adolph von Schell notes*,* "In our peacetime map problems, war games, and field exercises, we have simple solutions. There is no uncertainty, nothing goes wrong, units are always complete In war it is quite otherwise. There is no situation that our imagination can conjure up which even remotely approaches reality Therefore, if you would train for the realities of war, take your men into unknown terrain, at night, without maps and give them difficult situations Every soldier should know that war is kaleidoscopic replete with constantly changing, unexpected, confusing situations. Its problems cannot be solved by mathematical formulae or set rules."*[40]*

Developing future commanders who expect to be surprised and seek to surprise also supports the emphasis on campaigning in manoeuvre and modern management theories.[41] Surprise missions should be more readily given in exercises and readiness tests. The more units embark on non-set-piece training, the more confident they are when they are when operating in uncertainty. The US Army has recognised the value of such training in that at least a third of the time, battalions undergoing JRTC evaluations have to respond to something that they did not plan for.[42] The end result is a growing group of commanders and soldiers who are confident in working in uncertain and constantly changing operational environments.

As adversity may be an energising force for innovation and change, adventure training can develop a culture that is less fearful of change. Today, the SAF's adventure training helps individuals overcome fear, a condition normally experienced on the battlefield which cannot be really simulated in peacetime, or develop skills to build confidence.[43] Taken to a higher level, adventure training can be a tool to assist in developing a change culture, focussing on attaining a higher stage of behavioural change.[44] Properly conducted, it takes people out of their comfort zone, allowing them to see their potential in a different environment, thereby assisting in changing their paradigms about the future.

By developing stimulating and challenging training, military organisations can encourage people to challenge SOPs and "doctrinal templates", equipping their future leaders and soldiers psychologically to cope with the rapidly changing world of the future.

Strategy Five Leading the Change

Machiavelli has opined that "there is no more delicate matter to take in hand, nor more dangerous to conduct, nor more doubtful in its success, than to be a leader in the introduction of changes. For he who innovates will have for enemies all those who are well off under the old order of things, and only lukewarm supporters in those who might be better off under the new."[45]

Effective communication is an essential part of leadership. Sullivan, as US Army Chief, used 'yellow memos' to communicate with his senior leadership and give them a sense that they were each an important part of a special team.[46] The European Patent Office, with a flatter structure and high scientist representation, disseminates infor-mation successfully with an I.T. based system.[47] Regardless of the communication system adopted, people want to hear from the top and to give feedback. If a healthy communication process is established, people will be less susceptible to believe in unhealthy rumours that are rife, especially in times of change.

Leaders must also reinforce communications by deeds; otherwise cynicism and risk aversion will occur within the organisation. If management communicates one message and practises another, people quickly translate this contradiction into confusion, incompetence, or dishonesty.[48]

People make up an organisation's culture. The military demands more of them than any organisation in that they are expected to sacrifice their lives for the nation. The challenge for leaders, during uncertainty and change, is to constantly reassure their employees and create positive feelings about the future. While a selected few in the organisation can effectively thrive in change, a large majority cannot and there is a need as senior leaders to practise "servant leadership"[49] by caring for their employees to reassure and create positive feelings about the future. This means visiting and talking to people, especially those who are most affected by change, discussing their fears, offering assurance and most of all, just listening. By understanding people, and adjusting strategies to minimise resistance to change, leaders can win over those who are afraid and convert them to adopt the new organisational culture.

Leadership is fundamental to the implementation of a learning organisation that imbues a positive change culture. By communicating, grooming and caring for people effectively, leaders can win them over to the new transformational change culture.

Conclusion: Transformational Change A Vision for the SAF

Today's military, attuned to stability, need fundamental changes to operate effectively in a world of continuous change. Military culture's ability to adapt to the new paradigm is critical as cultural barriers can be potent obstacles to organisational change while change within a supportive cultural environment is accepted better and more likely to succeed.

This essay has developed five strategies that the SAF can adopt to create such a culture. Firstly, there is a need to anchor cultural change on strong values and vision. Secondly, we will need to foster creativity together with thirdly, the need to take risks and accept mistakes. Fourthly, effective training can facilitate cultural change. And finally, we need sound leadership to see through the changes. Working together, these strategies will provide a good basis on which the military 'control culture' is transformed into a "can-do, can-dream", "growing-learning" culture.[50]

With this new culture for transformational change, the SAF can look forward to the following - the perfect military culture is futurist, always endeavouring to envisage the "SAF After Next", whilst maintaining the strong continuity of its core values. It contains leaders with courage who champion innovation and change.

They strongly advocate defined risk taking and are prepared to assign time and resources to engineer change and actively demonstrate a willingness to tolerate, and even celebrate, failure. They delegate authority to solve problems and implement solutions, train and create teams that are compatible and trusting, and break down strategies into achievable objectives. Subordinates are encouraged to constantly improve their skills and often work outside their area of expertise in an environment of reduced uncertainty and increased confidence. The organisation calls innovation exploration, advocates constant learning, creates trust and makes it safe to dream big. A military culture such as this will be a champion of transformational change.

Endnotes

1 Stalin, J., quoted in Garthoff, *Soviet Military Doctrine,* 1953.

2 Moss Kanter, R. 1983, *The Change Masters: corporate entrepreneurs at* work, Unwin Hyman, London, Chapter 2.

3 Tushman, M.L. and O'Reilly, C.A. 1997, *Winning Through Innovation,* Harvard Business School Press, USA, p 220.

4 Conner, D.R. 1992, *Managing at the Speed of Change*, John Wiley & Sons Ltd, England, p 38 measures change in terms of these 3 variables and finds all 3 rising in the future; see also Toffler, A. 1980, *The Third Wave*, Morris, New York, pp 23-25.

5 Daft, R.L. 1997, *Management(4th Edition)*, The Dryden Press, Fort Worth, p. 746.

6 A good summary of the 'traps' which organisations fall into when trying to change can be found in Sullivan, G.R. & Harper, M.V. 1996, *Hope is not a method: what business leaders can learn from America's army*, New York, Times Business, Chapter 2 "The Paradox of Action".

7 Byrne, J. A. 1992, "Paradigms for Postmodern Managers", *Reinventing America*, Business Week, pp 62-63; Land, G & Jarman, B. 1992, *Breakpoint and Beyond*, New York, Harper Business.

8 Sullivan, G.R. & Harper, M.V. 1996, op cit, chapter 10.

9 Patton , G S Jr, 1931, "Success in War", *Infantry Journal*, Jan 1931.

10 Snider D.M. "An Uninformed Debate on Military Culture", *Orbis A Journal of World Affairs,* Volume 43, Number 1, Winter 1999, p 15.

11 Szafranski, R 1996, "Interservice Rivalry in Action", *Airpower Journal*, Summer 1996, pp. 48-59.

12 O. Dunivin, K. 1994, "Military Culture: Change and Continuity", *Armed Forces and Society*, Vol 20, No 4, Summer 1994, pp.531-547; Phelps, M.L. 1997, "The Australian Army's Culture: From Institutional Warrior to Pragmatic Professional", *ADF Journal*, No 123, March/April 1997, pp. 37-43.

13 Murray, W. 1999, "Does Military Culture Matter?", *Orbis*, Winter 1999, p 27.

14 Albrecht, K. 1994, *The Northbound Train: finding the purpose, setting the direction, shaping the destiny of your organisation*, AMACON, pp 22-24.

15 Senge, P 1990, *The Fifth Discipline: The Art and Practice of Learning Organisations,* New York, Doubleday, 1990, introduction.

16 Hamel, G & Prahalad, C. K. 1994, *Competing for the future*, Harvard Business School Press, pp 130-133.

17 See Nevis, E C , Lancourt, J, Vassallo, H G 1983, *Intentional revolutions: a seven-point strategy for transforming organisations*, Jossey-Bass, p 77-79.

18 *The SAF Core Values*, SAFTI Military Institute, Apr 1997.

19 Sullivan, G.R. & Harper, M.V. 1996, op cit, p 79.

20 Till, G. 1997, "Adopting the Aircraft Carrier", in *Military Innovation in the Interwar Period,* eds Murray, W. and Millett, A.R. 1997, Cambridge University Press, Cambridge, p 200.

21 Lim, C. 1999, "Setting Sights beyond 2000", *The Army News*, Issue 49, April 99, MINDEF, Singapore, pp. 1, 4-5.

22 Daft R.L. 1997, op cit, p 747.

23 Tushman, M.L. and O'Reilly, C.A. 1997, op cit, p 35.

24 Schein, E. 1995, "How can organisations learn faster? The challenge of Entering the Green Room", *Sloan Management Review*, Winter 1995, p. 89.

25 Senge, P 1990, *The Fifth Discipline: The Art and Practice of Learning Organisations,* New York, Doubleday, 1990, p 15.

26 Sullivan, G.R. & Harper, M.V. 1996, op cit, p 12.

27 Micklethwait, J. and Woolridge, A. 1997, *The Witch Doctors*, Random House, London, p. 147.

28 "Manpower Policies" supplement, *Pointer*, Feb 1982, p. 10.

29 Rhodes, J.E. 1998, "Every Marine an Innovator", *Marine Corps Gazette*, Jan 1998, pp 40-41.

30 Vandergriff, D.E. 1998, "Without the Proper Culture: Why our Army cannot practice Maneuver Warfare",*Armour*, Jan-Feb 1998, pp 20-24.

31 Schein, E. 1994, "Organisational and Managerial Culture as a Facilitator or Inhibitor of Organisational Learning", *MIT Organisational Learning Network Working Paper,* No. 10.004, 19 May 1994, p. 7.

32 Tushman, M.L. and O'Reilly, C.A. 1997, op cit, p 113.

33 Ulmer W.F. "Military Leadership into the 21st Century: Another 'Bridge Too Far?''', *Parameters*, Vol XXVIII, No.1, p 20.

34 Powell C.L. 1995, *A Soldiers Way*, Random House, New York, p 320.

35 Murray W. 1997, op cit, p34.

36 Murray W. 1997, op cit, p34.

37 Sullivan, G.R. & Harper, M.V. 1996, op cit, chapter 11.

38 Senge, P 1990, *The Fifth Discipline: The Art and Practice of Learning Organisations,* New York, Doubleday, 1990, p 14.

39 Sullivan, G.R. and Harper, M.V., 1996, op cit, p 48.

40 From: Captain Adolph von Schell's 1933 "Battle Leadership", cited in Lind, W.S., 1985, *Maneuver Warfare Handbook,* Westview Special Studies in Military Affairs, Westview Press, London, UK, p 65.

41 Sullivan, G.R. and Harper, M.V., op cit, p 127.

42 *JRTC Handbook*, 101st Airborne Division, US Army.

43 Moore, R.C. 1997, "The Role of Adventurous Training in the Australian Defence Force", *ADF Journal,* No. 123, Mar/Apr 1997, pp 45-47.

44 Brookfield, S.D. 1986, *Understanding and Facilitating Adult Learning*, Jossey-Brass, San Francisco, pp 212-214.

45 Tushman, M.L. and O'Reilly, C.A. 1997, op cit, p 36.

46 Sullivan, G.R. & Harper, M.V. 1996, op cit, chapter 12.

47 Binney, J & Williams, C 1995, op cit, p 75.

48 Tushman, M.L. and O'Reilly, C.A. 1997, op cit, p 223.

49 Senge, P. 1990, "The Leader's New Work: Building Learning Organisations", *Sloan Management Review*, Fall 1990, pp. 7-22.

50 "Prime Minister's National Day Rally Speech", *The Straits Times*, 22 Aug 1999 Singapore Prime Minister Goh Chok Tong argues that "can-do" is insufficient for future organisations: they need a "can-dream, can-do" culture.

Bibliography

Albrecht, K. 1994, *The Northbound Train: finding the purpose, setting the direction, shaping the destiny of your organisation*, AMACON

Brookfield, S.D. 1986, *Understanding and Facilitating Adult Learning*, Jossey-Brass, San Francisco

Byrne, J. A. 1992, "Paradigms for Postmodern Managers", *Reinventing America*, Business Week

Conner, D.R. 1992, *Managing at the Speed of Change*, John Wiley & Sons Ltd, England

Daft, R.L. 1997, *Management(4th Edition)*, The Dryden Press, Fort Worth

Garthoff, *Soviet Military Doctrine,*1953

Hamel, G & Prahalad, C. K. 1994, *Competing for the future*, Harvard Business School Press

***JRTC Handbook*, 101st Airborne Division, US Army**

Land, G & Jarman, B. 1992, *Breakpoint and Beyond*, New York, Harper Business

Lim, C. 1999, 'Setting Sights beyond 2000', *The Army News*, Issue 49, April 99, MINDEF, Singapore

Lind, W.S., 1985, *Maneuver Warfare Handbook,* Westview Special Studies in Military Affairs, Westview Press, London, UK

"Manpower Policies" supplement, *Pointer*, Feb 1982

Moore, R.C. 1997, "The Role of Adventurous Training in the Australian Defence Force", *ADF Journal,* No. 123, Mar/Apr 1997

Moss Kanter, R. 1983, *The Change Masters: Corporate Entrepreneurs at Work*, Unwin Hyman, London

Micklethwait, J. and Woolridge, A. 1997, *The Witch Doctors*, Random House, London

Murray, W. and Millett, A.R. (eds) 1997, *Military Innovation in the Interwar Period,* Cambridge University Press, Cambridge

Murray, W. 1999, "Does Military Culture Matter?", *Orbis*, Winter 1999

O. Dunivin, K. 1994, "Military Culture: Change and Continuity", *Armed Forces and Society*, Vol 20, No 4, Summer 1994.

Nevis, E C , Lancourt, J, Vassallo, H G 1983, *Intentional revolutions: a seven-point strategy for transforming organisations*, Jossey-Bass

Patton , G S Jr, 1931, "Success in War", *Infantry Journal*, Jan 1931

Phelps, M.L. 1997, "The Australian Army's Culture: From Institutional Warrior to Pragmatic Professional", *ADF Journal*, No 123, March/April 1997.

Powell C.L. 1995, *A Soldiers Way*, Random House, New York

"Prime Minister's National Day Rally Speech", *The Straits Times*, 22 Aug 1999

Rhodes, J.E. 1998, "Every Marine an Innovator", *Marine Corps Gazette*, Jan 1998

Schein, E. 1994, "Organisational and Managerial Culture as a Facilitator or Inhibitor of Organisational Learning",*MIT Organisational Learning Network Working Paper,* No. 10.004, 19 May 1994

Schein, E. 1995, "How can organisations learn faster? The challenge of Entering the Green Room", *Sloan Management Review*, Winter 1995

Senge, P. 1990, *The Fifth Discipline: The Art and Practice of Learning Organisations,* New York, Doubleday, 1990.

Senge, P. 1990, "The Leader's New Work: Building Learning Organisations", *Sloan Management Review*, Fall 1990

Snider D.M. "An Uninformed Debate on Military Culture", *Orbis A Journal of World Affairs,* Volume 43, Number 1, Winter 1999

Sullivan, G.R. & Harper, M.V. 1996, *Hope is not a method: what business leaders can learn from America's army*, New York, Times Business

Szafranski, R 1996, "Interservice Rivalry in Action", *Airpower Journal*, Summer 1996

Toffler, A. 1980, *The Third Wave*, Morris, New York

***The SAF Core Values*, SAFTI Military Institute, Apr 1997**

Tushman, M.L. and O'Reilly, C.A. 1997, *Winning Through Innovation,* Harvard Business School Press, USA

Ulmer W.F. "Military Leadership into the 21st Century: Another 'Bridge Too Far?'", *Parameters*, Vol XXVIII, No.1

MAJ Seet Pi Shen is a Guards Officer by training and is currently a Section Head at HQ Supply & Transport. He previously served as the S3 in a Singapore Infantry Brigade (SIB) HQ. He graduated with a BA (2nd Class Upper Honours) in Philosophy, Politics, and Economics from Oxford University in 1992 and obtained a Master in Defence Studies, University of Canberra, in 1999. He also attended the Australian Army Command and Staff Course (Fort Queenscliff) 1999. MAJ Seet won the first prize in the 2000 and 1999 CDF Essay Competitions.

The Professional Soldier

By CPT Lim Ann Nee

"It is just another job. It is the same no matter where you work!"

My mum

I signed on the dotted line at the tender age of 19, to serve the country for a minimum contract of eight years, in exchange for four years of sponsored study in UK. Three and a half years after working in the SAF, I still get asked by people why I sign on. When expounded, this simple question implies greater underlining meaning that can be extended to SAF's manpower issues. Essentially, it can be translated to, "Who will serve?"

The Singapore Army and the volunteer People's Defence Force, a part-time reservist force, were established after Singapore's independence in 1965. Recognising the urgency of creating a credible and deterrent military defence, the government began to step up recruitment and recruit training, and in Nov 1976, introduced the concept of conscription. Today, the SAF commands a strength of 350,000, of which 20,000 are regular officers and WOSEs, 30,000 conscripts and the rest NSmen.

As Singapore's economy strengthens over the years, the SAF has to face tougher and tougher competition for manpower resource from the private sector. Just like many Western counterparts, the reliance in recruiting and retaining regular service personnel is primarily based on monetary inducements guided by labour force realities. Unsurprisingly, the recruitment level of the SAF is negatively correlated to the condition of the economy higher recruitment during recession and vice versa. The manpower department faces the perennial problem of recruiting and retaining a sufficiently large number of regulars, particularly officers, to train and manage the SAF. In a bid to combat these problems, MINDEF attempts to offer its regulars increasingly attractive terms of service, including competitive salaries pegged to the "market rate". Manpower policies are also constantly reviewed to accommodate recruitment trends. Most recently, the SAVER plan, coupled with a better route-of-advancement scheme, was introduced to entice regular officers to serve longer in the SAF. As the recruitment and retention rate amongst the officers seemed to be driven more and more by extrinsic factors, the reasons for joining the service become obscured.

"I go anywhere in the world they tell me to go, any time they tell me to, to fight anybody they want me to fight. I move my family anywhere they tell me to move, on a day's notice, and live in whatever quarters they assign me. I work whenever they tell me to work And I like it. Maybe that's the difference."

From "A Country Such as This"

The military organisation has always been viewed as an institution, where its members are assigned with the sacred task of protecting the country and her people. The organisation is normally state funded and military personnel, particularly officers, command a certain level of respect and authority from the general public. In some countries like Israel, veteran status is virtually a pre-requisite for achievement in the civil society (Gal, 1986). However, many fail to realise that a voluntary armed force in a modern, democratic society is one that maintains its autonomy but also refracts societal trends; it does not function in isolation from the society. Military sociologists identify the social structure of the military organisation as one that moves along a continuum of scale (Moskos, 1977). On one end of the scale is an organisation that is strictly bounded by institutional concepts and on the other extreme end is one that is entirely determined by occupational concepts. A modern military organisation is deemed to be moving along the continuum of scale, from the institutional end towards the occupational segment, though the extent of occupational influence on the armed forces varies from country to country.

According to Moskos(1988), an institution is legitimated in terms of values and norms. Members of an institution are often seen as following a calling captured in words like duty, honour, country. To a certain degree, the institutional membership is congruent with notions of self-sacrifice and identification with one's institutional role. In return, institutional members enjoy a certain authority over, and esteem from the larger society. Military service has many inherent institutional features, like fixed/minimum terms of enlistment, liability for 24-hour service, subjection to military discipline and law, inability to resign (before end of contracted term) or change working conditions. The members tend to be generalists who will perform any job as assigned, including a range of operational and staff appointments. In addition, there are the physical dangers inherent in combat training and operations. A paternalistic remuneration system is also characteristic of an institutional military. Much of compensation is non-cash such as food, housing, uniforms, and medical benefits. Notions of overtime pay are also non-existent. Furthermore, while civilian compensation system is one in which marketability determines reward, remuneration in the military is traditionally based on rank and seniority.

An occupation, on the other hand, is legitimated in terms of the market place. The pay system is determined by the supply and demand of the market. Workers with equivalent skill levels and/or educational qualifications ought to receive approximately the same pay, regardless of the organisation. An occupation has also well-defined roles and the workers tend to be specialised in their jobs. Because the end-product of an occupational organisation is in the form of tangible profit, it is easy to determine a person's performance and thus, his salary, according to his productivity. In return, an individual's main motivation to work would generally be extrinsic factors, like his pay and promotion. The occupational model implies the priority of self-interest, rather than that of the organisation.

"The SAF is an armed force; it is not a civilian corporation. Its mission is to defeat its enemies, ruthlessly and completely."

BG Lee Hsien Loong, Sep 1984

While the military social structure is unique for every armed forces, it is evident that the SAF is gradually moving from an organisational format that is predominantly institutional to one that is becoming more and more occupational, either subconsciously with societal trends, or deliberately through manpower policies. Over the years, incremental developments slowly amount to profound changes. The volunteer armed forces is inevitably subjected to pressures for social change imposed by the societies in which they are immersed. The SAF must adapt and be flexible to remain relevant, especially if we want to continue to attract quality personnel from the market labour. Unfortunately, the tilt towards civilisation without re-enforcing institutional values may have undesirable effects on the service personnel and in turn affect our military effectiveness.

Firstly, there has been an increasing number of civilians working in MINDEF, filling up officer appointments that are non-operational in nature. These civilians, formerly known as NUSAF (Non-uniformed SAF), work in areas of finance, purchasing, logistics, personnel, policies, legal services and even intelligence analysis. NUSAF personnel are subjected to military law and the paternalistic remuneration system of the armed forces, but have more defined work roles and are not expected to uphold institutional values. In recent years, the NUSAF scheme has been replaced with the DXO (Defence Executive Officers) scheme in a bid to accommodate more occupational features of a free labour market.

The narrow definition of the work role among civilians can increase the workload of military personnel and create morale problems. For example, I recall an incident when a friend confided in me some manpower problems his department encountered. Due to unforeseen circumstances, his department was put on a 24-hour alert and all the officers (including civilians) were asked to do overnight duties. The civilians were upset as they did not think that the duties were within their workscope and requested to be exempted. However, the uniformed officers would need to do significantly more duties if the civilians did not share the workload and as officers, they could not reject the work. The incident created great morale problems within the department. Feelings of relative deprivation are unavoidable when the diffuse responsibilities of the military institution co-exist with the more limited work roles found in civilian occupations.

Another significant change in the military institution is seen in the more flexible manpower policies implemented. It is evident that manpower policies for the uniformed personnel are formulated based on *laissez-faire* principles. Monetary rewards are used as the mean motivation to attract recruitment. The paternalistic remuneration system is also evolving from the non-cash benefits to cash compensation. For example, whereas the officers used to stay in SAF housings/compounds, most of them are now given housing aid in the form of subsidised loans. Various medical and dental schemes in the form of cash rebates are also available for the regulars. Attempts are also made to tie an officer's salary scheme to his/her educational qualifications (i.e. the three schemes of pay, A/B/C), the type of work he/she specialises in (i.e. vocational allowance) and his/her work performance (i.e. performance bonus). These policies aim to alleviate recruitment and retention problems by re-defining military remuneration as comparable, if not better than civilian remuneration.

While it is necessary to consider individual needs in manpower policies, organisational developments can be seriously hampered when intrinsic motivations are replaced by extrinsic motivation. Extensive psychological research (Staw, 1976) has shown that inducing members to perform tasks with strong extrinsic rewards may create behaviour that will not be repeated except for greater extrinsic rewards. Moreover, extrinsic rewards can weaken intrinsic motivation. While monetary remuneration is important, it cannot replace the personal values and commitments required for a member to serve the country. The military organisation requires certain behaviour from their members that can never be made to serve individual interests, at least not in a narrow economic sense. Military effectiveness can be seriously undermined if the service personnel will not do more than what they are paid for.

In an attempt to stay relevant and maintain its effectiveness, MINDEF has also been promoting a corporate culture advocated in the commercial arena. Business lingos and ideas are not uncommonly expressed in the management of the organisational structure. Work processes like ISO 9000 and Singapore Quality Class frequently used in the private sector have also been adopted as assessments of quality and effectiveness of the organisation. On top of that, many sectors, particularly the logistical, technological and administrative sectors, that are traditionally managed by MINDEF have been contracted or privatised.

Corporate values advocate work attitudes and processes that are highly focused and effective, and encourage the worker to be innovative and bold in his/her approach to work. While many of these values are applicable to the military, one must not forget that the main motivation behind corporate values is profits profits to the organisation that may lead to higher pay for the individual. The success of the work process and the efficiency of the worker in a corporation can be easily assessed by the difference in the profit margin. However, cost-effectiveness should not be the principal concern in the business of defence. More often than not, the functions of our tasks cannot be weighed using monetary means. We must be cautious of assimilating occupational values into the military culture, and consciously make sure that the correct values are being cultivated to our service personnel.

The reliance on technologically advanced weaponry system necessarily equates to the requirement for highly skilled and trained operators. The operator, who is the soldier in this case, inevitably becomes more and more specialised, with more defined work scope as his/her job may not be easily substituted. The extensive use of technology renders the SAF susceptible to increasing specialisation and a diffused sense of purpose. In fact, Wood(1980) suggested that the airforce officer corps are most susceptible to occupational trends as they work with highly advanced weaponry and normally require relatively long training periods. Airforce officers, particularly pilots, seemed to identify increasingly with their civilian counterparts. The overall trend is away from those who identify themselves primarily as military officers and towards those who see themselves as specialists in uniforms, a movement from military professionals to professionals in the military.

"If you get the values right, than the other things fall into place."

Peters and Waterman, "In Search of Excellence", 1984

Although strategies for external integration is vital for the SAF to function effectively and essential to increase the numbers and quality of persons coming forward for military service, they fail to address the meaning of military service and the need to develop a coherent value system for its regular service personnel. As a result, the traditional perception of the military as a calling to the nation by her citizens, legitimated by broadly based national values, seem to be giving way to a subjective definition of the military service as an occupation in the labour market. Such a trend is perturbing because the military profession demands more of a soldier than any other job in the market place; the demands which cannot always be compensated in monetary terms. It will be unfair and certainly erroneous for me to speculate that the SAF will not be able to maintain its combat readiness and to fight and win a war simply because we no longer operate in the conventional way. On the contrary, the SAF needs to constantly re-invent itself to stay on top of and relevant to changes and demands of the military organisation. However, it is also undeniable that institutional values critical to accomplishing missions are giving way to self-centred priorities, a phenomenon which is clearly manifested in our recruitment and retention problems.

The challenge for military leaders in the new millennium is to articulate a definition of military service and a core value system that will cushion the undesirable influence from the occupational sector and enhance our service to the nation. Whereas the SAF was an important tool to achieve our political wills and to deter any hostile intent in the past decades, its role seemed to have evolved in this new century. The SAF is not only developing its capabilities in conventional warfare, it is also exploring new frontier in confronting Low Intensity Conflict. The way we fight a threat may have changed, but the intent has not we are protecting the sovereignty of our country. The traditional SAF core values must be inculcated in all service personnel and officers must lead by example in putting these values to practice. The move to promote soldiering as a profession must not neglect to specify the meaning of military service and set the scope and limits of role obligations for service members at all levels of the organisation. Most importantly, the SAF should emphasise the military career as one that is:

- nation-centred and not organisation-centred;
- mission-centred and not career-centred;
- group-centred and not individual-centred; and
- service-centred and not work-centred (Cotton, 1988).

The military profession is more than just a job. The professional soldier is one who puts the nation before oneself, and understands that his/her responsibilities cannot be entirely compensated by extrinsic rewards. He/She must be intrinsically motivated to serve the nation and her people, and must be willing to sacrifice himself/herself in times of necessity. The problems of recruitment and retention cannot be alleviated unless our soldiers understand the values behind military service.

This essay won a Commendation Award in the CDF Essay Competition - 2001.

Bibliography

1. Barry M. Staw, *Intrinsic and Extrinsic Motivation* Morristown N.J. : General Learning Press, 1976.

2. Charles A. Cotton, "The Institutional Organization Model and the Military," *The Military: More than Just a Job*, Pergamon-Brassey's International Defense Publishers, 1988.

3. Charles C. Moskos & Frank R. Wood, *The Military: More than just a job* Pergamon-Brassey's International Defense Publishers, 1988.

4. Charles C. Moskos, "From Institution to Occupation: Trends in Military Organisation", *Armed Forces and Society*, Vol. 4, No. 1, 1977.

5. Frank R. Wood, "At the Cutting Edge of Institutional and Occupational Trends" ***The Military: More than just a job*****, Pergamon-Brassey's International Defense Publishers, 1988.**

6. Reuven Gal, ***A portrait of the Israeli Soldier,*** **Conn.: Greenwood Press, 1986.**

CPT Lim Ann Nee is a Weapons Systems Officer (C3) by training and is currently a Staff Officer in HQ RSAF. She previously was a controller at an Air Force Brigade. She graduated with a BSc (1st Class Honours) in Psychology from University College London in 1997 and obtained a MSc Occupational Psychology from Nottingham University, UK in 1998. She won a Commendation Award in the 1999 CDF Essay Competition.

Cyber-Terrorism: An Emerging Security Threat Of The New Millennium

By CPT Ow Kim Meng

Terrorism in the world today is changing. The terrorist attacks on the US World Trade Centre on 11 Sep have clearly shown the world that new age terror makers are extremely capable of thinking "out-of-the-box" and exploiting any terror tactics or "weapons" to achieve their demented goals. In this age of information superhighways, the traditional paradigm of terrorism is evolving beyond traditional physical violence, hijacks and bombing. Today, a terrorist does not need to travel thousands of miles to attack a target. The terrorist does not need to risk detection during the long journey. Today, because of the networked nature of critical infrastructures in most countries, a terrorist does not need to risk attacking the target nation's military or government installations if they can much more easily attack its soft digital underbelly: Cyber-Terrorism.

While the world has yet to see an instance of large scale cyber-terrorism, cyber attacks by terrorists resulting in physical or psychological distress to targeted governments or civilian populations by disrupting critical systems will likely occur in the future.[1] Just as Osama Bin Laden and Al-Qaeda had caught the US, the mightiest military superpower in the world, by complete surprise with their "out-of-the-box" attacks, we must look beyond traditional boundaries in anticipating new terrorist threats that likely cannot be eliminated, only limited and managed. The defence and containment of these new emerging threats, including cyber-terrorism, will require well-orchestrated and closely co-ordinated efforts and commitment among civilian, intelligence, law enforcement and military organisations, both in-country and across the world.

The Emerging Threat of Cyber-Terrorism

In recent years, a great deal of attention has been paid to the vulnerability of critical infrastructures of a country in light of new cyber vulnerabilities. In many parts of the world today, including Singapore, the military and civilian sectors rely upon critical infrastructures to provide a variety of vital services ranging from telecommunications to emergency services, from financial transactions to military operations and government services. The critical infrastructures of modern society are underpinned by information servers and electronic networks, which enable their national and international access to governments, military and private operators. The dependence of modern society on computers and communications systems to support the day-to-day lives of society, power demands, finance and trade, and transportation systems places most of the modern society at risk in the event of a cyber attack.[2]

As a nation becomes more technologically advanced, it will also become inherently more vulnerable to such forms of cyber attacks.[3] Military strategists around the world fear that it may one day be possible to paralyse an entire nation by cyber attacks and prevent its autonomous involvement overseas. Cyber-terrorism, born from the information warfare genius, is beginning to evolve from a minimal threat associated with isolated attacks to a strategic threat, if co-ordinated with traditional tactics by state-sponsored rogues or organised terrorist groups in pursuit of a higher level agenda. Information warfare techniques utilised by such cyber-terrorists may prove advantageous and deadly in the hands of these pariah terror makers looking to take advantage of vital infrastructure vulnerabilities of modern society to create chaos. Cyber-terrorism, when used in conjunction with a state-sponsored terrorist campaign or antecedent to a state's war campaign, may conjoin to form a strategic threat in tipping over the balance of a war campaign in both the civilian and military sectors.

What is Cyber-Terrorism?

The US Department of Defence (DoD) defines cyber-terrorism as a criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of

services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social, or ideological agenda.[4] In this context, telecommunications capabilities refer to the specialised knowledge and skill used to manipulate telecommunications systems, thereby allowing individuals to obtain an extensive level of control over a penetrated system.

One of the distinguishing characteristics of cyber-terrorism is that it is the target that defines the nature of cyber-terrorism, not necessarily the means. For example, cyber-terrorism is any attack against an information function, regardless of the means. Installing a malicious code inside a public telecommunications switching facility is cyber-terrorism, if initiated by non-state or state-sponsored perpetrators. The physical destruction of a public telecommunications switching facility is also considered an act of cyber-terrorism.

Vulnerabilities of Modern Society to Cyber-Terrorism

Before dwelling further on the cyber terror threat, it is important for us to peruse the source of vulnerabilities in today's modern society that provide the strength in cyber terror fears. To this end, Singapore is a highly accurate symbolic reflection of a modern society. The strong dependence of Singapore's living standards on the vital services in the world indicates that any disruption in these services will be inconvenient, costly and even life-threatening. 36 years ago when Singapore first became independent, a prolonged island-wide power disruption would only have affected a small fraction of the well-to-do population and probably a small handful of commercial and government entities. Fast forward to present day, such an outage and its impact would be disastrous and extremely costly. Another vital vulnerability of Singapore, or any modern nation, is the telecommunications infrastructure. The backbone of our nation's financial mechanism, one of the most vital functions of any modern nation, hinges largely on the complex web of telecommunications network coaxial landlines, fibre optics trunk lines, wireless linkages, satellite stations, switches, exchanges spanning our entire island and linking us to the world beyond. A major disruption of these vulnerabilities could severely affect the integrity of our national defence operations, our economy and the integrated services of Singapore's infrastructures. In particular, if fallen prey to such attacks, the SAF would find itself in an extremely unfavourable position, because:

- Interconnectivity is needed for the conduct of modern military operations.
- There is widespread utilisation of commercial products, communications infrastructures, and complex commercial software (may be collectively referred to as COTS).
- Interoperability with joint and multi-national coalitions mandates the use of broadly accepted commercial standards.

The factors listed above are by no means complete, and they are not confined to Singapore or the SAF. These seemingly independent and disjointed factors often form the fracture points that may be wedged apart to create a plethora of "Achilles heels" within modern society. Once compromised, these vulnerabilities may be exploited by anyone with the means and appropriate tools including cyber-terrorists, members of national intelligence organisations, information warriors, criminals, industrial competitors, hackers, and aggrieved or disloyal insiders. What is it that makes us so vulnerable to such attacks?

The world's economy and communications networks are integrating at a staggering pace. Informed estimates by experts suggest that 90 to 95 percent of the information needed to carry out essential governmental functions must in some way be processed by information systems in the privately owned and operated parts of the national information infrastructure. Such a trend can be clearly found within the Asian region. With Asia's rise as an "info power" after experiencing an explosion in economic growth in the late '80s and '90s, and a similarly rapid expansion in the use of communications and information technologies, access to telephones across the region has increased dramatically in the past decade. According to the United Nations World Development Report (UNWDR), in 1990 there were only six telephone lines per 1,000 people in India, eight in Pakistan, less than one in China, six in Indonesia, 10 in the Philippines, 24 in Thailand, 89 in Malaysia and 385 in Singapore. By 1998 the statistics had changed dramatically, with the

number of lines per 1,000 people rising to 222 in India, 19 in Pakistan, 70 in China, 27 in Indonesia, 37 in the Philippines, 84 in Thailand, 198 in Malaysia and 562 in Singapore.[5] The same trend is also occurring in other countries around the world. With the entire world getting increasingly reliant on such telecommunications infrastructure, the world is also providing cyber-terrorists with a powerful conduit to hold an entire nation, or even the world, hostage.

Another potential area of stranglehold that may be effectively exploited by cyber terror makers is the ever-growing online trend of the world. In Asia alone, there are increasing numbers of people going online. Over 18% of the world's 319 million registered Internet users are from Asia. Within a short span of three years from 1997 and 2000, the proportion of online population in Singapore has grown from a 14.7% to 50%. The trend is even more staggering in China, the country with the largest population in the world. The online population of China has expanded from a measly 0.0001% to 1.34% during the same period. This figure may seem insignificant, but when translated to headcounts, it represented an increase in 16.9 million people! By 2005 the world's online population is expected to rise to 24%.[6] As the information age progresses, the entire world is growing increasingly interlinked to one another. The emerging integration of transcontinental and national network services connected to critical infrastructures is increasingly making the world a more vulnerable target to cyber-terrorist attacks. This arena is further inflamed by the proliferation of advanced technologies and weapons systems including nuclear, chemical and biological that may be employed effectively by rogue countries and organised terror groups such as Al-Qaeda to launch physical attacks on a target nation's information and cyber infrastructures.

Why Use Cyber-Terrorism?

There are many advantages to using cyber-terrorism against an adversary who is technologically superior. Such an adversary is likely to be more critically dependent on information-related systems and strategies and more vulnerable to their disruption *vis-à-vis* a backward nation. From the cyber-terrorist's perspective, cyber-terrorism can abet operations meant to deter or defeat traditional military threats stemming from technologically superior adversaries at relatively low costs. Cyber terror may also act as a force multiplier and enable terrorist operations to concentrate resources in other areas or on other targets. Cyber-terrorism offers terrorists five critical advantages that may compel such perpetrators to utilise the cyber battleground. They are:

- Low entry costs, especially when compared to the costs of conventional military hardware;
- Immediate and unexpected action there is no time for the victim to act if caught either unaware or unprepared;
- Veil of anonymity;
- Global reaches; and
- Little risk for the individual sitting at the keyboard - attackers can be located anywhere provided they have access to a network through which they could launch their information assault on the desired target.

Weapons and Tactics of Cyber-Terrorism

One of the greatest challenges for us in the light of this emerging threat is the capability to identify a cyber-terrorist attack as it is happening. Presently, it is nearly impossible for most countries, including the US, to detect cyber terror or information warfare attacks in progress due to the lack of such capabilities. Attacks are usually discovered after they have been completed and the damage has been wrought. Most cyber-terrorist acts will go undetected or untraceable. For example, several hackers broke into US military computers during the Gulf war and eluded identification for four days. During this period, the US military did not know who was attacking key defence computers essential to deploying forces to the Persian Gulf.

Fortunately in this episode, the hackers were teenagers, not Iraqi forces.[7] Cyber attacks can be conceived and planned without any detectable logistic preparation. These attacks can be invisibly reconnoitred, clandestinely rehearsed, and then mounted in a matter of minutes or even seconds without revealing the identity and location of the attacker. Cyber-terrorism will become a strategic threat to a nation's security if the terrorists are able to identify a means of attacking vital assets and disrupting them in such a way that the damage prevents a nation from effectively deploying its military forces to defend its interests.

Cyber-terrorism will take on various forms and tactics, depending on the perpetrators and their objectives. Cyber-terrorism is not limited to attacks on cyber assets or attacks originating in cyberspace, but also includes physical attacks on facilities that support cyber operations. Cyber terror weapons and attacks may be computer generated or rely on more conventional assaults employing truck bombs, poison gas attacks, explosives, or cable cutting to unleash a chain of events in which a power service grid, gas pipeline, or air traffic control system collapses in a cascading effect. Traditional weapons may also be employed to launch attacks against the target nation's information systems. However, the cyber aspect of cyber-terrorism has received a great deal of attention in recent years. A former director of the CIA had said "the electron, in my view, is the ultimate guided weapon." Information infrastructure can be attacked through the application of cyber-terrorism in five mediums[8]:

- Through corrupted system hardware or software;
- Through electronic jamming devices;
- Through the use of an insider;
- By means of an external hacker; and
- By physical attack.

Some forms of such cyber software weapons employed for the purpose of disrupting the information infrastructure include:

- *Computer Viruses*
- *Logic Bombs*
- *Trojan Horses*
- *Worms*
- *Sniffer or Electronic Eavesdropping Programs*
- *Next Generation Automated Computer Hacking Tools*

Having examined the various forms of cyber terror weapons, let us examine some examples of the possible cyber terror tactics[9]:

- Remotely accessing the processing control systems of a cereal manufacturer to change the levels of iron supplement of the cereal for the purpose of sickening and killing the children of a nation;
- The disruption of banks, international financial transactions and stock exchanges, causing the people of a country and foreign investors to lose all confidence in the target nation's economic system;

- Attacking a target nation's air traffic control systems to cause two large civilian aircraft to collide. Much of the same can be done to the rail lines and domestic mass transit system;

- Remote alteration of the formulas of medication at pharmaceutical manufacturers. The potential loss of life is unfathomable;

- Remotely changing of the pressure in the gas lines, causing a valve failure and a gas pipe explosion. Likewise, the electrical grid is also vulnerable to such attacks; and

- Remotely overriding of a heavy chemical manufacturing plant's internal safety monitoring systems, thereby leading to the devastation of the plant and the contamination of the plant's surrounding area with hazardous chemicals.

In effect, such acts of cyber-terrorism can make certain that the population of the target nation will not be able to eat, drink, move, communicate or live. In addition, the people charged with the protection of their nation including the military, law enforcement agencies and other homefront protection agencies - will not have any warning prior to the attacks. Neither too will they be likely to be able to shut down the cyber-terrorists, since they would most likely be on another part of the world. In the networked world of today, the effects of such cyber attacks could spread far beyond the radius of a bomb blast. The new technological innovations of the information revolution of the new millennium have opened up a Pandora's Box of exploitable vulnerabilities for the entire world.

Deterring Cyber-Threat

How can we plan to deter a phenomenon that cannot be detected, has real-time striking ability, may be misrepresented under the guise of false-flags and can be caused by either an internal malfunction, hacker, cyber-terrorist or foreign adversary? Many experts in this field have suggested that proper cyber-terrorism deterrence should be limited to an Information War response, or response in-kind. Others have proposed for the mitigation of a nation's vital vulnerabilities by switching all its vital assets to separate isolated and secured computer networks. As the arena of cyber-terrorism is a relatively new emerging form of security threat, there are few countries and security/military organisations that we may draw references and lessons from. However, there are several elements of Information Warfare that would probably prove to be effective in deterring cyber-terrorism. One such element is Psychological Operations (Psyops). Psyops use a variety of methods such as misinformation to affect the enemy's reasoning. A terrorist organisation capable of launching a cyber attack could be bombarded with e-mails detailing a caveat against cyber-terrorism attacks and adumbrating retaliation that would guarantee their destruction. Counter cyber-terrorism operations could also be disseminated through their computer resources. Psyops may also assist in deterring cyber-terrorism by manipulating the potential cyber-terrorists' computer, financial and internet resources to such a degree that they may feel it is in their best interests not to employ cyber-terrorism as a means to their ends.

Another effective form of deterrence to cyber-terrorism is the employment of Electronic Warfare (EW). EW can include tactical operations against terror forces via the Internet or through any electronic means of communication. For example, the US had employed varied forms of EW to eavesdrop on the activities of Osama Bin Laden through his mobile phone communications after the 11 Sep attacks. The US had also employed EW and Information Warfare techniques to detect, trace and disrupt international money transfers and other financial activities of Muslim activists who supported the suspected terrorist groups.

Security measures form an important deterrence to cyber-terrorism because they reject efforts to corrupt the integrity of military and civilian assets through cyber attacks. Effective security measures keep the adversary from learning about the target nation's true capabilities and intentions. Current security measures include OPSEC (Operations Security), COMSEC (Communications Security) and COMPUSEC (Computer Security). Obviously, the most effective means of negating the threat of cyber-terrorism is to have a well-defended information infrastructure that is impervious to cyber attacks. To this end, the tools of Information Warfare provide an effective means to deal with cyber-terrorism. Furthermore, Information War operations and the advanced technologies that make a nation more vulnerable are also the best tools of deterrence

that may promote its defence if used effectively. Certainly, improved intelligence collection and assessment, as well as modern information processing and C2 capabilities will be critical in any successful deterrence against would-be aggressors.

An effective deterrence policy used to combat cyber-terrorism should involve a wide range of multi-faceted responses, including military operations and retaliations. Such possibility of retaliatory actions will contribute to the deterrence of attacks by instilling the idea of "an eye for an eye". Certainly, cyber-terrorists would be less willing to wage cyber-terrorism operations if they thought the consequences for such attacks would mean the destruction of their assets, resources, and potentially, their existence. The message of the will and ability to carry out retaliation must be credible and unwaiverable to achieve the best effect of deterrence.

Conclusion

The face of terrorism is changing in the new millennium. While the motivations remain the same, the world is now facing new and unfamiliar means of waging terror, one of which is cyber-terrorism. The existing intelligence systems, tactics, security procedures and equipment that were once expected to protect people, systems, and nations, are generally powerless against this new emerging form of terror. Cyber-terrorism may serve as a vital element to terrorist strategy because as a force multiplier, cyber-terrorism may provide terrorists with an additional resource to cause disruption of critical infrastructures and other strategic assets without having to deploy their operators. As can be seen from the 11 Sep attacks, even a military super-power such as the US can be "stung" by surprise and suffer grievous civilian and economic consequences, much less the rest of the world.

In the face of this new emerging form of security threat of the new millennium, we must develop the capability to deny, detect, and deter cyber-terrorism without sacrificing any vital infrastructures or military credibility. As technology continues to proliferate, cyber-terrorism is likely to mature in this new century. If cyber-terrorism policy, deterrence and response capabilities are not developed to meet ongoing technological advances in civilian industry, then the world may find itself paralysed in responding to a looming international security threat.

This essay won a Commendation Award in the CDF Essay Competition 2001.

Endnotes

1 "New (or innovative modifications of old) forms of warfare are emerging and will likely be employed in the future." & " Transnational Infrastructure warfare, attacking a nation's key industries and utilities; telecommunications, energy and power, transportation, governmental operations and services, emergency services, financial, manufacturing, etc.", web article *Global Threats And Challenges: The Decades Ahead*, Lieutenant General Patrick M. Hughes, USA, Director Defense Intelligence Agency, 1998.

2 "The Pentagon is already planning advanced forms of information warfare, including computer-based sabotage of an enemy's computing, financial and telephone systems before a shot is fired in anger.", web article *The New Canons Of War - Chronicles Of The Future*, C Stewart, 1999.

3 "HI-TECH nations such as Australia could be threatened by terrorism and warfare waged through the Internet ", web Article *Australia: Www Wired For War, J Masanauskas, 1998*

4 Extracted from *US DoD Report* on "Cyberterrorism: An Evolving Concept" (Published 2001), Pg 2.

5 Statistics on Asian telecommunications growth extracted from web Article *Asia - Grasping Information Warfare, 2000*.

6 Statistics on Asian online population growth extracted from web article *Asia - Grasping Information Warfare, 2000.*

7 Based on account of incident published in web Article *Cyber Wars, Wars Of The Future*... TODAY, Jun 1999.

8 Information obtained from web Article *GLOBAL THREATS AND CHALLENGES: THE DECADES AHEAD*, Lieutenant General Patrick M. Hughes, USA, Director Defense Intelligence Agency, 1998.

9 Information extracted from web article *The Future Of Cyberterrorism*, Barry C. Collin, 1999.

Bibliography

1. "Cyberwar is Coming", *Strategic Review*, Vol 12, 1999.

2. "The Strategic Implications of Information Dominance" , *Strategic Review*, Vol 22, 2000.

3. "The Information Revolution and Warfare 2020", *Defence News*, March 1999.

4. "Information Warfare and the Air Force: Wave of the Future? Current Fad?", *RAND*, March 1996.

5. "Report Urges Info System Safeguards", *Defence News*, March 1997.

6. "Cyber-terrorism", *Foreign Report*, September 1997.

7. "Cyber wars", *The Economist*, 13 January 1996.

8. "Defense Technology", *The Economist*, 10 June 1995.

9. "*National Security in the Information Age*", Devost Matthew, 1995.

10. "Russian Views on Future War", *Jane's Intelligence Review*, September 1998.

11. "Russian Views on Electronic Signals and Information Warfare", *American Intelligence Journal*, May 1994.

***12. Information Warfare at the Crossroads*, Frederick Brian E, 1997.**

13. "The Future of Warfare: Select Enemy. Delete", *The Economist*, 08 March 1997.

***14. The Data Weapon*, Grier Peter, June 1998 3rd edition.**

***15. Information Warfare and Deterrence*, Harknett Richard J, 1996.**

16. "Information Warfare: A Two-Edged Sword", *RAND*, November 1998.

17. "Desert Storm: The First Information War", *Airpower Journal*, Winter 1994.

***18. Information-Age Warriors*, Byte, July 1992.**

***19. Defensive Information Warfare*, Albert David S, 1996.**

***20. Computers under Attack: Intruders, Worms and Viruses*, Deming Peter, 1995.**

***21. Information War*, Lewonowski, Mark C, 1993.**

***22. What is Information Warfare?*, Libicki Martin C, 1995.**

***23. Sun Tzu and Information Warfare*, Neilson Robert E, 1997.**

***Information Warfare: Chaos on the Electronic Superhighway*, Schwartau Winn, 1994.**

CPT Ow Kim Meng is a Weapons Systems Officer (C3) by training and is currently a Staff Officer at HQ RSAF. Previously he held the appointment of controller at a Squadron. He graduated with a BEng (1st Class Honours) in Computing and a MSc in Advanced Computing from the Imperial College of Science, Technology and Medicine - London. He won a Commendation Award in the 1998 CDF Essay Competition.

The Motivations and Methods of the Terrorist

by MAJ (NS)(DR) Aaron Chia Eng Seng

"Terrorism is the violence that negates violence. Terror in fact is fraternity. For terror is my guarantee that my neighbour will stay my brother; it binds my neighbour to me by the threat of the violence it will use against him if he dares to be 'unbrotherly'. Now, terror is not only fraternity; it is also liberty."

Sartre[1]

"If you know the enemy and you know yourself, you need not fear the results of a hundred battles."

Sun Tzu[2]

Many countries have their share of terrorist attacks. Consider Karadzic's or Milosevic's equally insane "ethnic cleansing" and terrorist purges in Bosnia and Kosovo in the 1990s. The British have dealt with exploding trucks and buses ignited by Irish Catholic nationalists, and the Japanese with nerve gas placed in Tokyo subways by members of a Hindu-Buddhist sect. In India, residents of Delhi have experienced car bombings by both Sikh and Kashmiri separatists. The US suffered a bomb blast in the Olympics in Atlanta in 1996, and aerial attacks on the World Trade Centre in New York and the Pentagon in 2001. The Israelis and Palestinians have confronted the deadly deeds of both Jewish and Muslim extremists.

Why do the terrorists carry out these attacks? In this essay, the author strives to understand the mind of the terrorist, how they can morally justify what they did, the political and cultural contexts that produces these acts of violence, and the strategies, tactics and weapons they use.

Definition

"One person's terrorist is another person's freedom fighter."

The word "terrorist" comes from the Latin root word *terrere* meaning "to cause to tremble." The designation of terrorism is a subjective argument about the legitimacy of certain violent acts as much as it is a descriptive statement about them. "If the world is perceived to be peaceful, violent acts appear as terrorism. If the world is at war, violent acts may be regarded as legitimate. They may be seen as pre-emptive strikes, as defensive tactics in the ongoing battle."[3] For example, the US has been accused of terrorism in the atrocities committed during the Vietnam War and there is some basis for considering the nuclear bombings of Hiroshima and Nagasaki as terrorist acts.[4]Thus, to the attackers, whoever stands by a just cause cannot be called a terrorist.[5] On the other hand, the diverse origins and semantic justifications of terrorist acts are irrelevant to the victims.[6]

Causes and Motivations

"To die as a suicide bomber is better than to die daily in frustration and humiliation."

Abdul Aziz Rantisi[7]

It is difficult to separate causes from conditions, reasons and motives for the existence and development of terrorism. In fact the four are so intertwined in reality that to separate them may be futile. The underlying causes and motivations of terrorism can be studied at three levels: individual, national or group and international.

- ## Individual

At the individual level, human traits and certain psychological drives may motivate people to resort to terrorism. Some simply see madness as the cause for recourse to terrorism.[8]Others developed the theory of frustration-aggression.[9] The discrepancy between demand and fulfilment drives the individual to aggression, which may be expressed in physical violence to the extreme of terrorism. Some terrorists are just criminals. One of the theories put forward by psychiatrists and criminologists to explain why so many German women were involved in urban guerrilla activities is that it provides them with a form of liberation.[10] Because they are from good homes and are well educated, they consider themselves superior to men and want to display that superiority in action.

There are those who join to find their identities by becoming part of the group. They commit acts to feel accepted. Because of the need to belong to the group, they seldom resign or compromise their involvement. Some joined for money, some for therapy, some for excitement. Others were attracted by the combination of excitement and the possibility of drugs and sexual indulgence. Culturally motivated terrorists are willing to do anything to defend their language, religion, group membership or native homeland especially if the rewards are high in this world or the next. Sometimes, the families of these terrorists are held hostages to ensure their commitment to the cause.

Rev Michael Bray defended the need to kill and if necessary to die over the issue of abortion. According to him, there has been a great cosmic war going on - the confrontation between the good and evil - one that goes unseen largely because the enemy has imposed its control.[11] His view is that Americans have a disregard for human life and a penchant to kill. These religious struggles can be perceived as a defence of basic identity and dignity and losing the struggle would be unthinkable. When the struggle cannot be won in real time or in real terms, it is elevated to the cosmic plane through terrorism, where it will be in "God's hands". In spiritualizing violence, religion has given terrorism power. Suicide bombers see themselves as religious sacrifices and hope to be richly rewarded in heaven.

Leaders of terrorist groups are usually politically minded. Some leaders have even made the successful transition from terrorism to political leadership while keeping their terrorist organizations intact, for example, Yasser Arafat.[12] These leaders usually received better than average educations and often come from prosperous families. They have the conviction that they can impose their beliefs on others. They use the philosophers to provide them with a persuasive rationalization for their actions.[13] Some come under the influence of political thinkers who preach that violence is essential to make the world a better place for the masses. Eakman characterized Osama Bin Laden's relationship with his chief mentor, former psychiatrist Ayman al Zawahiri as: "It would not be the first time psychiatrists had served as manipulators, systematically feeding their hatreds, stroking their egos, and stripping their consciences, until eventually even the most barbaric act may appear plausible and rational in the name of some twisted cause."[14]

It takes a community of support and in many cases, a large organizational network for an act of terrorism to succeed.[15] It also requires an enormous amount of moral presumption for the perpetrators of these acts to justify the brutal attack on another life, especially the life of someone one scarcely knows and against whom one bears no personal enmity. It requires social acknowledgement, and the stamp of approval from a legitimising ideology or authority one respects. Because of the moral, ideological and organisational support necessary for such acts, most of them come as collective decisions.

- ## National or Group Level

At the national or group level, specific conditions of the state and of the social system may provoke people to terrorism. Relative deprivation of basic needs that occurs on the individual level can be a factor in uniting a group of people. Hardship may be a cause of terrorism, along with urban growth,

and "moral explosion".[16] The existence of a tradition of violence (as in Latin America) is usually conceived as a catalysing factor of terrorism as well as a reaction to it. Huntington postulated that young males are the perpetrators of violence in all societies; their overabundance in Muslim societies is one of the causes for the rise in the number of Islamic terrorists.[17]

Terrorism often becomes a useful tool in the tolerant liberal states, which are vulnerable to it. Severe repression, or under-reaction, implying incompetence on behalf of the reacting government may both attract and encourage further terrorism.[18] The evolution of the modern political terrorism is historically parallel to the development of the liberal state.[19]Terrorism evolved at the same rate as liberal ideas were expanding. First there is anarchist terrorism that is associated with the concept of the "propaganda of the deed". This advocates the propagation of the anarchist message among the masses by terrifying governments and people, so as to bring about a revolutionary atmosphere of socio-political insecurity.[20] Among the ideologies of revolution, Maoism provides a basis for a great deal of justification for terrorism.[21] Maoism has had a great influence on Western New-Leftists as well as modern anarchist terrorism and, especially, on terrorists of the Third World.[22]Trotsky once said: "Terror can be very efficient against a reactionary class which does not want to leave the scene of operations."[23]

Nationalist, ethnical-separatist aspirations and revolutionary movements compose the next category. Of these organizations, the Irish Republican Army (IRA), the Euzkadi Ta Askatasuna (ETA, Spain), etc, all make use of the terrorist method. The Israelis succeeded in setting up their own state through the use of the terror weapon. Indeed the Israeli Prime Minister, Menachem Begin, was once leader of Irgun Zvi Leumi who blew up King David Hotel in Jerusalem, killing 89 military and civilian personnel.[24] The Palestinians can also be considered as "territorial terrorists". To them, Palestine means the whole of Palestine, and they want to recover that land from Israeli possession and to control it themselves. There is also the revolutionary terrorist seeking to change the socio-political scene (Japanese Red Army, Red Brigades, fascist movements in Italy, Turkey, etc).

Rarely if ever is religion the major cause of war, but it is often a critical factor. Faith serves to legitimate, motivate and increase intensities, whether promoting or protesting war. Religions routinely legitimize violence and contribute to it through their theologies, rituals and organizations.[25] From earliest wars of conquest to colonial wars and contemporary ethnic conflicts, religion is at the core of war making.[26] Many religious terrorist groups are labeled as fundamentalists. However, not everyone who takes his religion seriously is a fundamentalist. These fundamentalists or "religious warriors" are not motivated by religious sensibilities; rather, they exploit religious fervor for their own irreligious ends. A fundamentalist believes that circumstances require him to act politically and probably violently to fulfill his religious obligations.[27] Many fundamentalists are often well-educated people. Yet they feel strongly that Western society erred grievously when they replaced God, religion and divine law with human reason and secular political principles as the basis for the legal and social order.[28]

Jewish, Christian or Muslim fundamentalists are selective in choosing certain scriptures or theological teachings from the past and insisting that true believers "fight to the death" (literally and figuratively) to protect these "fundamentals". Their pattern of thought is absolutist (the truth we proclaim is perfect, complete and irreformable); inerrantist (free from any kind of error); and dualist (we are children of light while others are children of darkness).[29] Fundamentalists also believe that they are living in a special time in history, perhaps in the last days. In the final days, when these believers find themselves in direct combat with the enemy, they retrieve teachings that justify violent action in defence of the faith.

The initial motivations for groups to resort to terrorism may be simple. However, later rationalisation may blur their motives. Some Palestinian groups, for example, have developed a commitment to world revolution almost as total as their devotion to the recovery of their homeland. The past support of the Soviet Union for almost any group that could embarrass the West,[30] whatever that group's political alignment, blurred the picture even more. Nowhere could there be more confusion than in the welter of reasons the Provisional IRA gives for its campaign of

terror: national, political, social and religious causes mixed together provide them with their rationalisation.

- ## International Level

At the international level, confusion within the global system facilitates the development of terrorism. As a cheaper type of warfare involving few clearly definable risks or international responsibility, it has become more convenient for states to have recourse to the services of individual terrorists, supported by various groups and conversely, for groups to resort to terrorism as a result of the support they receive. These transnational terrorist groups do not act on behalf of any particular state; membership and resources are drawn from supporters in more than one state; and the area of operations, including targeting, transcends state borders. Examples of such groups are those that provide fighters for religiously motivated wars around the world (such as the Balkans and Chechnya) and those targeting certain countries (such as US and Israel).

According to the *RAND Chronicle of International Terrorism*, the US headed the list of countries whose citizens and property were most frequently attacked since 1968. There are many reasons for this. In its role as trading partner and political ally, the US has a vested interest in shoring up stability of regimes around the world. It is a common refrain among America's critics in the Middle East that the US props up objectionable local leaders out of selfish interests.[31] For example, to protect its access to oil the US supports repressive princes in the Persian Gulf states. This also puts her as a defender and promoter of secular governments, raising strong objections by religious opponents. Others viewed the US as meddling in their domestic affairs according to her own interests. Carlos Marighella wrote in his handbook of guerrilla warfare: "Kidnapping American personalities who live in Brazil, or who have come to visit here, is a most powerful form of protest against the penetration of US imperialism into our country."[32]

America is so comfortable with its own brand of capitalism and consumer culture that it cannot fathom just how revolutionary these forces can be.[33] Americans tend to believe that their institutions and values democracy, individual rights, the rule of law and prosperity based on economic freedom appeal to all cultures. Furthermore, the US's success as the sole global superpower may encourage animosity and resentment more than admiration, including contempt for US culture as a threatening export especially in the form of alcohol and sexy movies. For example, the commercial success of Hollywood films is often judged as a political or cultural threat, from Paris to Kabul. Unfortunately the US also fails to realize that its culture of individualism clashes with some of the collective customs of these countries.

The impact of globalisation (of which the US is the leader) is perceived by some states as cultural encirclement, or a new form of dependency and colonialism. Fundamentalist movements of a religious, ethnic, or communal nature strive on these feelings.[34] According to Osama bin Laden, there is a holy war between Islam and America. His hatred stemmed from American foreign policy in the Middle East. He believes that the US military presence in Saudi Arabia defiles Muslim holy land. He is offended by continued sanctions against Iraq, Syria, Sudan, Libya and Iran. He also objects to America's substantial support of Israel. He blames the US for the killing of Bosnian Muslims by Christian Serbs because of a UN arms embargo against Bosnia until 1994. The symbolic attacks on the World Trade Centre (economic), Pentagon (military) and the failed attempt on the White House (political) can be seen as a defiant act by the terrorists to tell the world what the US has been doing to them. Although Osama's motivations may appear to be religiously motivated, other factors such as political (e.g. US foreign policy and repressive governments in the Middle East), cultural (e.g. individualism and American values), and economic (e.g. globalisation) play important roles.

Strategy, Tactics and Weapons

"To secure ourselves against defeat lies in our own hands, but the opportunity of defeating the enemy is provided by the enemy himself."

Sun Tzu[35]

The strategy for terrorists encompasses the following:[36] First, the act must be horrifying, striking at innocent lives that have nothing to do with the cause the terrorists are espousing; second, it provokes uncertainty and is directed against the society as a whole and does not distinguish civilians and military targets; third, it depends and uses the mass media to communicate and publicise its acts and motives. The use of violence is obligatory in order to induce fear and chaos and it is aimed at the people and the institutions of the established order.[37] Violence provides the glue that binds terrorists together into a unity of purpose even for those who are violently opposed to one another. They also aim to make themselves into heroes and so persuade opponents and neutrals that the terrorists' cause is righteous and their actions are justified.[38] Their strategy is to make the other party appear in the wrong or be guilty of brutality. In religiously motivated terrorism, "Satanization" has been used to de-legitimise an opponent.[39]

Terrorists today are better organized, more professional and better equipped. They are prepared to take greater operational risks,[40] including death. Their delivery methods include suitcases, commercial vehicles or couriers, public transportation systems, private vehicles in land, sea and air. The most devastating asymmetric attacks on civilians in North America, Europe and Japan to date have not relied on military platforms for delivery. They make use of complex terrain, novel tactics and technology (hit and run tactics, fighting in large urban areas where the identification of attacks is hindered by large numbers of civilian bystanders and where counter attacks carry the risk of further civilian casualties). While the US is talking on the synergistic nature of remote fires, precision engagement, battlefield awareness and information dominance, the asymmetric actor will see the synergistic nature of terror, deceit, brutality and unpredictability. The terrorists have the following weapons at their disposal: the mass media, technology, psychology and drugs, and sabotage.

- ## The Mass Media

  An important variable in determining the scope of success of a terrorist assault is the mass media. Since terrorism is a violent method aimed at the psychological effect of the deed, the mass media, which occupies a determinant position in the formation of public opinion, becomes a useful tool for any terrorist act. Terrorism enjoys high ratings among the world's TV viewers and terrorists revel in massive exposure.[41] One of the best examples of the use of publicity by urban guerrillas was the Olympic games massacre at Munich in 1972; they had made the rest of the world aware of the Palestinian cause. Although not a direct cause of terrorism, the media, nonetheless, serve as an accelerator for the spread of the phenomenon and as a factor in the choice of tactics. Without the assistance of the modern mass media, terrorism would probably be significantly reduced.[42] The effect of the mass media on terrorism depends very much on the tone of the media discouraging or encouraging it.[43]

  The mass media is a perfect tool for terrorists, providing their services free of charge. It sometimes assists the terrorist's long-term objectives by supporting terrorism, specific terrorist causes and acts, and by opposing government, police or the judiciary. [44] Often the media tends to focus on the background of poor oppressed groups, defining their recourse to terrorism as "freedom fighting" or "guerrilla warfare." This provides an important service in building up the terrorist image and legitimising the terrorist's method.[45] Moreover, there is wide media coverage of detained or freed hostages testifying to the human treatment received from the terrorists. This too, is a precious and conscious component of terrorist strategy.[46] Some careless media may divulge plans of suppression that the terrorists can use to their advantage.[47]

The contribution of the mass media to the production of violence is a well-known theme of sociological and psychological research.[48] It also encourages the rapid appearance of numerous terrorist groups.[49] Irresponsible media coverage may encourage the adoption of terrorist tactics by common criminals. Exaggerated and widespread mass media coverage of terrorism has destructive effects on the social order i.e., the sensitivity of the moral judgement of the terrorist act is blunted and may prompt the terrorist to resort to even more spectacular acts to re-stimulate the public demand for expanded media coverage. Moreover, repeated false information may transform into "subjective truth".

- ## Technology

The developments in technology enable a single terrorist to be extremely destructive. For example, the advent of the jumbo jet has provided the terrorist with the ideal target. Once terrorists are able to threaten the flight crew, they have virtually achieved victory. Not only can the terrorists blow everybody in the aircraft to pieces, they may use the jet as a weapon to target densely populated areas. Weapons of mass destruction (WMD) such as biological, chemical and radiological agents make the killing of thousands of people relatively easy and are thus considered by many to be the most serious terrorism threat. They inflict mass casualties, cause terror and degrade morale. It is also possible for some of these weapons to be produced by individuals, a factor which increases the scope of the potential threat.

- ## Psychology and Drugs

Terrorists also use psychological warfare to support the achievement of objectives. They create fear, flood the market with an addictive or lethal drug, or create chaos through organized crimes that would weaken the country. They could also focus their attacks on politically influential sectors of the populace such as high-level officials, parents (by attacking children) and entertainment elite and celebrities.

Psychiatry or psychiatric treatments have also been employed to facilitate the execution of totalitarian and terrorist objectives. The Japanese *kamikaze* pilots in World War II used psychiatric drugs called amphetamines to get charged up.[50] In the 1980s, such pills were provided for suicide bombers in the Middle East[51] and they underwent "psychological indoctrination" intended to motivate them to move past the "point of no return".[52] Around the world, some 250,000 children, some as young as seven, have been used for armed combat.[53] The Human Rights Watch reported in 1999 "child combatants armed with pistols, rifles and machetes actively participated in killings and massacres, [and] severed the arms of other children Often under the influence of drugs, they were known and feared for their impetuosity, lack of control and brutality."[54]

- ## Sabotage

These attacks include destroying railroad stations, airports, loading areas, destroying high-value aircraft with short-range standoff weapons and damaging communications or intelligence facilities. Incendiary devices may also be used. Economic disruption is another tactic including attacks on means of production, the produce itself and on commercial infrastructure. Other forms of attack focused on the environment include attacks on chemical plants, power stations and waste-disposal sites in order to cause massive and dangerous pollution; destroying oil pipelines; poisoning water supplies; sinking oil tankers off the coasts; or spreading highly contagious diseases to crops or livestock as an adjunct to biological warfare. Food agents such as salmonella, foot-and-mouth disease and mad-cow disease can set off waves of poisonings.

Conclusion

Terrorism will continue to flourish. As long as extremists believe that violence is the only way to achieve their political aims, terrorism will continue on a greater or lesser level depending on passion engendered by their causes and the success of counter-terrorist forces. The Taliban regime in Afghanistan may be destroyed, but there will be more Talibans and new Osamas.

The "an eye for an eye" approach to terrorism usually fails especially if governments themselves resort to terrorist tactics. Any response to the perpetration of violent acts in the form of retaliation will enhance the credibility of the terrorists within their own community. The terrorism war can only be won by winning hearts and minds as well. This can only be achieved by correcting the historical mistakes made by those who unwittingly promote terrorism (repressive governments and international politicians), by being more sensitive to different cultures and religions and by ensuring future foreign policies of the major players in global politics will not create more terrorism. The recent US withdrawal from the 1972 Anti-Ballistic Missile (ABM) Treaty could unleash a new nuclear weapons build up,[55] perhaps making it easier for terrorists to obtain radiological materials. Secularism, democracy, and modernization take time to develop, especially when seen in the context of individualism, possible moral degeneration and religious corruption.

It is the author's sincere hope that through understanding the mind of the terrorist, responses to terrorism will not produce more terror, and anti-terrorism and counter-terrorism measures can be more effective.

Endnotes

1 Maurice Cranston, "Sartre and Violence,' Encounter, Jul 1967, p21.

2 Sun Tzu, James Clavell, ed. *The Art of War* (Hodder and Stoughton, 1981), p26.

3 Mark Juergensmeyer, *Terror in the Mind of God: The Global Rise of Religious Violence* (University of California Press, 2001).

4 *Ibid*.

5 Yasser Arafat at the UN General Assembly, 1974, as quoted by Secretary of State George Shultz in a speech in New York, 25 Oct, 1984.

6 Office of Technology Assessment, Chapter 3, 5 Dec 2001, p15. <http://www.wws.princeton.edu/~ota/ns20/alpha_f.html>

7 Dr Abdul Aziz Rantisi, Interview with Mark Juergensmeyer, Gaza, 1 Mar 1998.

8 Walter Laqueur, *Terrorism*, (London: Weidenfeld and Nicolson, 1977), p134.

9 John Dollard *et al*, *Frustration and Aggression*, (New Haven: YUP, 1940), p190.

10 Christopher Dobson and Ronald Payne, *The Terrorists: Their Weapons, Leaders and Tactics*, (New York: Facts on File, 1982), p52.

11 Juergensmeyer, *op cit*.

12 Dobson and Payne, *op cit*, p39.

13 *Ibid*., p18.

14 Beverly K. Eakman, *Cloning of the American Mind: Eradicating Morality Through Education*, (Huntington House, 1998).

15 Mark Juergensmeyer, *op cit*.

16 Laquer, *op cit*., p140-148.

17 Samuel P. Huntington, "The Age of Muslim Wars", *Newsweek*, Dec 2001-Feb 2002, p12. 18 Felix Gross,*Violence in Politics*, (The Hague: Mouton, 1972), p97.

19 Naomi Gar-Or, *International Cooperation to Suppress Terrorism*, (Australia: Croom Helm Ltd, 1985), p21.

20 *Ibid*.

21 Jayantanuja Bandyopadhyaya, *Mao Tse-Tung and Ghandi: Perspective on Social Transformation*, (Bombay: Allied Publishers, 1973), p31.

22 Gal-or, *op cit*., p19.

23 Kautskey, *Terrorism and Communism*, (New Park Publications, 1975), p78-79.

24 Dobson and Payne, *op cit*., p37.

25 Robert Wuthnow, ed. *Encyclopedia of Politics and Religion*, (Washington D.C.: Congressional Quarterly Inc, 1998), p770-774.

26 *Ibid*., p783-789.

27 *Ibid*., p280-288.

28 *Ibid*.

29 *Ibid*.

30 Dobson and Payne, *op cit*., p187.

31 Massimo Calabresi, Aisha Labi, Nicholas Le Quesne, Rebecca Winters and Yuri Zarakhovich, "Roots of Rage",*Times*, 1 Oct 2001 p42-44.

32 Carlos Marighella, *For the Liberation of Brazil*, (Harmondsworth, 1971).

33 Fareed Zakaria, "The Roots of Rage", *Newsweek*, 15 Oct 2001, p17.

34 Ali E. Hillal Dessouki, "Globalization and the Two Spheres of Security," *Globalisation and Politics*, 5 Dec 2001. http://www.globalpolicy.org/g;pna;oz/politics/ polit1.thm .

35 Sun Tzu, *op cit*.

36 Gar-Or, *op cit*., p5.

37 Dobson and Payne, *op cit*., p179.

38 *Ibid*., p3.

39 Juergensmeyer, *op cit*.

40 Office of Technology Assessment, *op cit*., p15.

41 *Ibid*., p13.

42 Jose M. Desantes Guanter, "Relationship between Freedom of the Press and Information and Publicity given by the Mass Media", *Conference on Defence of Democracy Against Terrorism in Europe: Tasks and Problems*, Nov 1980, p12-14. 43 Juan Tomas De Salas, "Responsibility of the Press and Other Information Media with Regard to Terrorism", *Conference on Defence of Democracy*, 1980, p7.

44 Norman Podhorez, "The Subtle Collusion", *The Jerusalem Conference on International Terrorism*, (Jonathan Institute, Jul 1979), p22-27.

45 Gernot Steinhilper, "Violence and the Police", *The Police and the Prevention of Crime*, 1979, p82.

46 Midge Decter, "The Need for Clarity", *Terrorism and the Media*, p6.

47 "Discussion Paper and Documentation", *The Jerusalem Conference on International Terrorism* (Jonathan Institute, Jul 1979), p21.

48 Larsen, *op cit.*, p15.

49 Otto N. Larsen, *Violence and the Mass Media*, (New York: Harper and Row, 1968), p. ix-293.

50 "Cutting through the Global Drug Network", *Sinorama*, Vol. 21. No. 4, Apr 1996.

51 Gordon Thomas, Journey into Madness, (London: Corgi Book, 1989), p27.

52 Erica Goode, "A Day of Terror: The Psychology", *The New York Times*, 12 Sep 2001.

53 Vivienne Walt, "Trained to Kill and Growing in Number", *The Washington Post*, 28 Feb 1999.

54 Douglas Farah, "Children Forced to Kill", *The Washington Post*, 8 Apr 2000.

55 Louise Branson, "US Storming of Ship Raises Spectre of Unilateralism", *Straits Times*, 15 Dec 01, p32.

MAJ (NS)(DR) Aaron Chia Eng Seng is a Air Operations & Communications Officer (AOCO) by training and served in numerous appointments at HQ RSAF. He is currently a Project Manager at DSTA. He has a PhD in Electrical Engineering (2001), MSc in Electrical Engineering (1998), MBA in Management of Technology (1995) and BEng (1989). He won the 1st prize and a merit award in the 1996 CDF Essay Competition.

When States May Lawfully Resort to Armed Force

by Ms Ong Yen Nee

In spite of an international mechanism such as the United Nations Charter to promote peaceful conduct of inter-state relations, post-war states still resort to armed force against each other in the conduct of their international relations. Post-war independence which led to the emergence of numerous new states, further complicates the already complex state of international affairs. Article 2(4) of the UN Charter stipulates that:

"All members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state or in any other manner inconsistent with the Purposes of the United Nations."

Thus, states are obliged not to resort to the use of force in the conduct of their international relations. This obligation, established in Article 2(4) and customary international law, may be considered a rule of jus cogens.[1]

Nevertheless, there are two important exceptions to Article 2(4) where the use of force is permitted, namely the right of self-defence and UN expressed authority. To discourage the return to "self-help" and unilateral use of force, the UN Charter has Article 51 on the right of self-defence, which sanctions the use of force.

First, the essay will discuss Article 51 where the use of force in self-defence is lawful. Under Article 51, there are two types of self-defence, namely individual and collective self-defence. Individual self-defence, based on State practice since 1945, will be discussed. This includes anticipatory self-defence, protection of nationals abroad, assertion of legal rights, and armed reprisals. Then collective self-defence will be discussed.

Second, the paper will highlight the other situations which are used by states to justify their resort to armed force. State practice over the years has shown that within the broad concept of self-defence, states justified their use of armed force on grounds of intervention (humanitarian intervention and intervention by invitation) and self-determination. In discussing these concepts, references will be made to state practice since 1945.

Third, besides the right of self-defence under Article 51, states may resort lawfully to armed force under the expressed authority of the UN, for purposes such as collective security and UN enforcement action.

Fourth, the unilateral use of force is regulated by both the UN Charter and customary international law. The use of force in self-defence can be evaluated on the principles of necessity, immediacy and proportionality. That is, these criteria can be used to assess whether the use of force is legitimate. Hence, these criteria merit a brief discussion.

To conclude, it will emerge from the following discussion that the right of self-defence is often broadly interpreted and invoked by states to justify their use of force. In view of the undesirable consequences of the use of force, its usage should be closely regulated and permitted only if it follows a "narrow" interpretation of Article 51 or has the expressed authority of the UN.

Self-Defence

States may resort lawfully to the use of armed force under Article 51 of the UN Charter, which specifies that:

"Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a member of the United Nations, until the Security Council has taken the

measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security."

Article 51 defines three important criteria for the use of force in self-defence, namely,

- the occurrence of an armed attack;
- the target (must be a "member of the United Nations"); and
- a "reporting clause".[2]

However, Article 51 is open to interpretation and states often interpret broadly the concept of self-defence so as to justify their actions. This gives rise to controversies regarding the exercise of the right of self-defence.

Anticipatory Self-Defence

The most controversial of the abovementioned three criteria is the first one on occurrence of armed attack, which gives rise to the concept of "*anticipatory self-defence*". Anticipatory self-defence refers to defence against *imminent* armed attacks,[3] that is, pre-emptive strike before the enemy has actually attacked (strike first in anticipation of an attack in future). The controversy is whether anticipatory self-defence is permitted under Article 51. Some argued that the words of Article 51 "if an armed attack occurs" mean that the armed attack *has to occur* before using force in self-defence.[4] This interpretation thereby renders the right of anticipatory self-defence unlawful. But the supporters of anticipatory self-defence "claim that Article 51 does not limit the circumstances in which self-defence may be exercised; they deny that the word 'if', as used in Article 51, means 'if and only if'".[5]

Controversies aside, the right of anticipatory self-defence had been invoked by a number of states, sometimes accepted but more often than not, rejected. One such case is Israel, which invoked this right when it bombed a nuclear reactor in Iraq in 1981, but was condemned by the Security Council.[6] Israel claimed that the reactor was used to make bombs which would be used against it; thus it was "entitled to destroy the reactor as an act of anticipatory self-defence".[7] A separate case which was endorsed was the 1986 US bombing of Libya; in which the US invoked the right of anticipatory self-defence "against acts of state-sponsored terrorism" to justify its bombing of Libya.[8] The controversy was revived again by the 1993 US missile strike on Iraq. The US justified the missile strike on grounds of "self-defence in response to an *actual* armed attack but also to further, *anticipated* armed attacks against it by Iraq".[9] Kritsiotis also commented that the US missile strike satisfied the other two criteria of self-defence, namely, the target of armed attack and the reporting clause.[10]

Right to Protect Nationals

M. Akehurst argued that the use of force to protect nationals abroad constitutes a form of self-defence.[11] He equated an armed attack on nationals abroad with that on the state itself, since it is the population that makes up a state.[12] It is controversial whether Article 51 permits the use of force in this situation; it depends on one's interpretation of the article.

The right to use force to protect nationals may be justified on two grounds:

- the use of force to protect nationals is a form of self-defence;

- it is "a right exempt from Article 2(4) because it is not (and does not compromise) 'territorial integrity or political independence'".[13]

An example whereby the alleged use of force to protect nationals abroad is legal is the 1976 Israeli rescue mission at Entebbe Airport, Uganda, which involved the use of armed force to rescue its nationals held hostage abroad.[14] Another more controversial case is the *Icelandic Fisheries Case* between Iceland and Britain. Known as the "Cod War" in the late 1950s and early 1960s, British vessels were used "to protect the asserted right of the British trawlers to fish in the disputed zone".[15] Britain justified its use of force in the "Cod War" as its right to protect its nationals fishing in the disputed zone.

Assertion of Legal Rights

There are situations when states justify their use of force on grounds of the right to assert their legal rights. The question is whether it is "lawful for a state to use a degree of force in the assertion of its legal rights".[16] In the 1946 *Corfu Channel Case* between Britain and Albania, the British warships, struck by Albanian mines when exercising its right of innocent passage in travelling through the North Corfu Strait, sent additional warships to "sweep the minefield".[17] The Court rejected Albania's claim that British display of force is a violation of Albania's sovereignty, as neither Albania's territorial integrity nor political independence was affected.

Armed Reprisals

It is believed that reprisals and self-defence are two different forms of self-help; self-defence is permissive, reprisals are not and are "punitive in character".[18] Reprisal is adopting a defensive nature taking the form of counter action. Reprisals "seek to improve reparation for the harm done, or to compel a satisfactory settlement of the dispute created by the initial illegal act, or to compel the delinquent state to abide by the law in the future".[19] Thus, reprisals short of the use of force may be lawful, but not armed reprisals.[20] Hence, self-defence excludes the right of armed reprisal.[21] Furthermore, in 1970, the General Assembly declared that "States have a duty to refrain from acts of reprisal involving the use of force."[22] This is evident from the Security Council's occasional condemnation of Israel for its armed reprisals against its Arab neighbours. The International Court of Justice (ICJ) also noted in its *Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons (1996)* that armed reprisals are unlawful.[23] An example is the Security Council's deploration of the UK's bombing of Fort Harib in 1964.[24]

Collective Self-Defence

The right of collective self-defence has not been clearly defined. The controversy is whether the right of collective self-defence is a collective exercise of individual rights of self-defence; or it is "the exercise of a right by one or more states on behalf of the 'attacked' state".[25] Adopting the latter definition, the North Atlantic treaty and other treaties defined collective self-defence as "each party undertakes to defend every other party against attack."[26]

In the 1986 *Nicaragua Case*, the ICJ said that "one state may not defend another state unless that other state claims to be (and is) the victim of an armed attack and asks the first state to defend it."[27] It also stressed that "for one state to use force against another, on the ground that that state has committed a wrongful act of force against the third state, is regarded as lawful, by way of exception, only when the wrongful act of provoking the response was an armed attack."[28]

In the case of the Gulf war, the US and its allies justified their use of force on this notion of collective self-defence. They had deployed forces in response to Kuwait and Saudi Arabia's requests for assistance after the Iraqi invasion of Kuwait. First, the deployment of forces to the Middle Eastern States was on the basis of "invitation by the governments concerned".[29] In the event of an attack on one of these states, the right of collective self-defence would render the use of force in response to the attack legal. Second, the use of force to remove Iraq from Kuwait was justified on grounds of right of collective self-defence. The British and

American governments contended that as such, there was "no legal requirement for them to obtain Security Council authorisation before embarking upon such an operation".[30]

Nevertheless, the legal basis for the use of force could be interpreted from the preamble to Resolution 678 (adopted by the Security Council on 29 Nov 1990), which stated that the Security Council was acting under Chapter VII of the UN Charter.[31] Thus, as a form of collective self-defence, the use of force in the Gulf was lawful.[32]

Intervention

International law does not have clear rules to govern the use of force by foreign intervention in civil wars. General Assembly Resolution 2131 (XX) provides that:

"No State shall organise, assist, foment, finance, incite or tolerate subversive, terrorist or armed activities directed towards the violent overthrow of the regime of another state, or interfere in civil strife in another State."

Thus, as a general rule, no state has a right to intervene in the internal affairs of another state.

An example is the 1986 *Nicaragua Case*, where the ICJ upheld that the US had violated the principle of the prohibition of the use of force and illegal intervention in the domestic affairs of Nicaragua through it aiding the contras who were rebelling against the government of Nicaragua.[33]However, the "specific scope of the prohibition of the indirect use of force under Art 2(4) of the Charter has still remained unclear with regard to assistance given by a foreign state to the 'private' use of force against another state."[34] Having said this, nevertheless, there are two types of intervention, namely, humanitarian intervention and intervention by invitation, where the use of force may be justified on grounds of self-defence, though they are controversial.

- ### Humanitarian Intervention

  State practice in general does not favour the concept of humanitarian intervention in view that "it might be used to justify interventions by more forceful states into the territories of weaker states."[35] State practice also points towards the tendency to justify the use of force on humanitarian grounds. A case in point was NATO's use of force against the Federal Republic of Yugoslavia in the Kosovo crisis. The objective of humanitarian intervention has been declared as the "protection of individuals and groups of individuals against their own state".[36]

  There are arguments for and against the use of force to achieve this objective. For instance, it can be argued for the use of force in intervention to "prevent and suppress large-scale violations of human rights".[37] It can also be countered that intervention on humanitarian grounds is "non-permissive", as it appears to violate Article 2(4) and various resolutions of the General Assembly such as GA Resolution 2131 (XX) (as stated in the preceding paragraph). An example is the Kosovo crisis, in which NATO (through the UK) tried to justify its use of force on grounds of "the right of humanitarian intervention in customary international law".[38] NATO action in Kosovo did not have a UN mandate. Thus, it was generally regarded as a "unilateral use of force justified (but justifiable?) on the basis of humanitarian intervention".[39]

- ### Intervention by Invitation

  In general, a state may invite external states to intervene in its civil war. "Intervention by foreign states in wars of national liberalisation would be lawful only if it could be shown that the national liberation movement (or the people whom it claims to represent) was the victim of an armed attack."[40] "A legitimate government may invite the forces of another state on to its territory for any purpose lawful under international law, that is, not for genocide, wars of aggression, or to prevent an exercise of self-determination etc."[41] Thus, the use of force can be lawful if one can prove that

one has been invited to intervene. That is, use of force in intervention by invitation is legal. An example is the US and Allied Forces deployment of troops to states in the Middle East following Iraq's invasion of Kuwait. However, the use of force in intervention by invitation also gives rise to two problems; namely, it may serve to "encourage dictatorial interference" by other states or it may be a "fabricated invitation", as in the case of the Soviet Union in Afghanistan in 1979 and the US in Grenada in 1984.[42]

Self-Determination

The principle of self-determination refers to "the right of a people living in a territory to determine the political and legal status of that territory".[43] Developing states supported the "alleged right of 'national liberation movements' to use force to achieve self-determination, and the alleged right of other states to assist them with force to achieve this objective."[44] However, this alleged right to use force is controversial and has not been legitimised by the UN Charter. The General Assembly Declaration of 1970 only provides that "every state has the duty to refrain from the use of force to deprive such peoples of their right of self-determination."[45] It follows that any assistance to help a state to "frustrate self-determination" is equally illegal.[46] Thus, the use of force to prevent self-determination is unlawful but there is nothing that endorses the use of force to achieve self-determination. In view that Article 2(4) propounds states to conduct their international relations through peaceful means, the use of force to achieve self-determination is likely to be unlawful. The right of self-determination does not entail the right to use force to achieve this goal, although self-defence has often been used as "justifications for the use of force by national liberation movements".[47]

Necessity, Immediacy and Proportionality

Customary international law stipulates that the use of force in self-determination must be "necessary, immediate and proportional to the seriousness of the armed attack".[48] The "necessity of the use of armed force is perceived and evaluated by the target-claimant and incorporated in the pattern of its expectations which, in the particular instance, impels the claim to use intense responding coercion."[49] Thus, the question of necessity of the use of force lies in the hands of the state. In the case of the 1993 US missile strike on Iraq, the US justified its action on the principle of necessity, that it was "*necessary to respond* to the attempted attack and the threat of further attacks by striking at an Iraqi military and intelligence target that is involved in such attacks."[50]

The principle of immediacy "requires that the act of self-defence must be taken immediately subsequent to the armed attack".[51] This implies that there should not be "an undue time-lag between the armed attack and the invocation of self-defence".[52] It is argued that a "determination of the 'necessity' for force is therefore an essential precondition to an examination of the immediacy of that force".[53] The purpose of the immediacy requirement is to prevent abuse under the "pretext of self-defence".[54]

Despite this, the evaluation of self-defence using this criterion takes into account the uniqueness surrounding each case. In the case of the 1982 Falkland Islands war, "although almost a month passed before British forces were prepared to counter attack, in view of the geographical distance, Britain's response was *immediate* by ordering the Royal Navy to leave for the area of conflict."[55]

The principle of proportionality requires that "any self-defensive measure should be quantified by the scale of the unlawful act which provoked it."[56] It is believed that "excessive force" would "jeopardise the legality of any operation undertaken in self-defence".[57] An example of disproportionate self-defence measure is Israel's seven-day bombing of South Lebanon in Aug 1993 in response to random rocket attacks on northern Israel by Hizbollah.[58] In its judgement on the *Nicaragua Case*, the ICJ stated that "there is a specific rule whereby self-defence would warrant only measures which are proportional to the armed attack and necessary to respond to it, a rule well established in international law."[59] Having said this, sometimes the determination of whether the use of force is proportionate may not be clear-cut.

Authorisation by the UN

Under the UN Charter, states may lawfully resort to force under the expressed authority of the UN for purposes such as collective security and peacekeeping. Collective security refers to the collective use of force under the authority of a "competent international organisation", usually to benefit the entire international community.[60] The power to exercise the collective security is vested in the UN Security Council, under Chapter VII of the UN Charter. The Security Council first determines based on Article 39 whether there has been a "threat to the peace, breach of the peace or act of aggression". Then it may invoke measures such as economic, diplomatic or military or a combination of sanctions. For example, diplomatic and economic sanctions (non-military sanctions) were imposed on Libya for the bombing of a Pan Am flight, known as the*Lockerbie Case*. The power to impose and terminate sanctions is in the hands of the Security Council. Both must be done by resolution.

- ## Regional Arrangements

  Article 53(1) states that "the Security Council shall, where appropriate, utilise such regional arrangements or agencies for enforcement action under its authority. But no enforcement action shall be taken under regional arrangements or by regional agencies without the authorisation of the Security Council." Thus, the UN has the right to authorise regional organisations "to use all necessary means including force to achieve a stated objective".[61]An example is the joint military action in the Korean conflict in 1950 and more recently, in East Timor, among others. However, regional organisations do not have the power to use force in enforcement action unless expressly authorised by the UN. In view of this, NATO action in the Kosovo is not lawful as it did not have UN authorisation.

- ## UN Peacekeeping

  There is nothing in the present UN Charter on peacekeeping missions. It was probably never perceived then that UN would have a peacekeeping role. UN peacekeeping involves the monitoring of ceasefires and the patrolling and maintenance of buffer zones. This operates under the UN mandate, preferably with the consent of the government. It takes two forms, one is simply peacekeeping whereby the operations are usually non-combat, undertaken to maintain or facilitate the achievement of peace between the warring parties.

  The other type of peacekeeping involves "peace enforcement", which refers to "operations involving the use of threat of force to preserve, maintain or restore international peace and security or to deal with the breaches of the peace or acts of aggression; these operations are authorised by the Security Council under Chapter VII of the Charter and do not require the consent of the states or other parties involved."[62] Under peace enforcement, which is authorised by the Security Council, the use of force is legitimate. The use of force is also legitimate in self-defence in peacekeeping operations. However, the line between peacekeeping action and enforcement action is rather blurred. Examples of UN Peacekeeping missions include the India-Pakistan border, in Sinai and the Golan Heights in the 1970s in the former Yugoslavia Republic of Macedonia (UNPREDEP), to name but a few.

Conclusion

To conclude, Article 2(4) prohibits the use of force with two exceptions, the right of self-defence (individual and collective self-defence under Article 51) and expressed authority of the UN for collective measures (including collective security, liberate territory and enforcement action). The use of force on the basis of self-defence is often broadly interpreted by states to justify their actions. Besides, states also try to justify the use of force on grounds of humanitarian intervention, intervention by invitation, and self-determination. Having said all these, as a general rule expounded by the UN, states should seek peaceful co-existence and refrain from the use of force in the conduct of their international relations.

Endnotes

1 Martin A Dixon and Robert McCorquodale, *Cases and Materials on International Law* (London: Blackstone Press, 2000) (3rd edition), p. 561.

2 D. Kritsiotis, 'The Legality of the 1993 US Missile Strike on Iraq and the Right of Self-Defence in International Law', *International and Comparative Law Quarterly*, Vol. 45, 1996, pp. 171-4.

3 Ibid., p. 171.

4 Peter Malanczuk, *Akehurst's Modern Introduction to International Law* (London: Routledge, 1997) (7th edition), p. 311.

5 Ibid., pp. 311-312.

6 Ibid., p. 313.

7 Ibid., p.313.

8 Ibid., p. 313.

9 D. Kritsiotis, 1996, p. 171. See also p. 172, the Clinton administration's argument that the Iraqi role in the assassination plan as an "actual armed attack" seems a bit weak.

10 Ibid., pp. 173-4.

11 See M. Akehurst, (1976/77).

12 Ibid.

13 Ibid.

14 Peter Malanczuk, 1997, p. 315.

15 Katz, 'Issues Arising in the Icelandic Fisheries Case', *International and Comparative Law Quarterly*, Vol. 22, 1973, p. 88.

16 Ibid., p. 87.

17 See ICJ Report 1949 4.

18 See D. Bowett, 'Reprisals Involving Recourse to Armed Force', 66 *AJIL* (1972) 1.

19 Ibid.

20 MN Shaw, International Law (Grotius: Cambridge, 1997) (4th edition), p. 786.

21 Peter Malanczuk, 1997, p. 316.

22 Ibid.

23 Ibid.

24 MN Shaw, 1997, p. 786.

25 Martin A Dixon and Robert McCorquodale, 2000, p. 575.

26 Peter Malanczuk, 1997, p. 318.

27 Ibid., p. 318.

28 MN Shaw, 1997, p. 795.

29 C Greenwood, 'Iraq's Invasion of Kuwait: Some Legal Issues', *World Today*, Vol. 47, 1991, p. 41.

30 Ibid.

31 bid., p. 42.

32 Ibid. However, as a form of enforcement action, the use of force was unlawful because the British and American did not have Security Council's authorisation before their military operation.

33 Peter Malanczuk, 1997, p. 319.

34 Ibid., p. 320.

35 MN Shaw, 1997, p. 802.

36 R. Lillich, 'Forcible Self-Help by States to Protect Human Rights', 53 Iowa LR 325 (1967-1968).

37 Martin A Dixon and Robert McCorquodale, 2000, p. 579.

38 D. Kritsiotis, 'The Kosovo Crisis and NATO's Application of Armed Force against the Federal Republic of Yugoslavia', *International and Comparative Law Quarterly*, Vol. 49, 2000, p. 340.

39 Martin A Dixon and Robert McCorquodale, 2000, p. 580.

40 Peter Malanczuk, 1997, p. 338.

41 bid., p. 581.

42 Ibid., pp. 581-582.

43 Peter Malanczuk, 1997, p. 326.

44 Martin A Dixon and Robert McCorquodale, 2000, p. 585.

45 Ibid., p. 584.

46 Peter Malanczuk, 1997, p. 337.

47 H. Wilson, 'International Law and the Use of Force by National Liberation Movements' (1989), pp. 130-136.

48 Peter Malanczuk, 1997, p. 316.

49 D. Kritsiotis, 1996, pp. 166-7.

50 Ibid., p. 167.

51 Peter Malanczuk, 1997, p. 317.

52 D. Kritsiotis, 1996, p. 168.

53 Ibid., p. 169.

54 Peter Malanczuk, 1997, p. 316.

55 Ibid., p. 317.

56 D. Kritsiotis, 1996, p. 170.

57 Ibid., p. 170.

58 Peter Malanczuk, 1997, p. 317.

59 Ibid., p. 317.

60 Martin A Dixon and Robert McCorquodale, 2000, p. 585.

61 http://www.un.org/Depts/dpko/dpko/intro/enforce.htm.

62 Martin A Dixon and Robert McCorquodale, 2000, p. 599.

Bibliography

1. Peter Malanczuk, *Akehurst's Modern Introduction to International Law* (London: Routledge, 1997) (7th edition)

2. Martin A Dixon and Robert McCorquodale, *Cases and Materials on International Law* (London: Blackstone Press, 2000) (3rd edition)

3. D. Kritsiotis, 'The Legality of the 1993 US Missile Strike on Iraq and the Right of Self-Defence in International Law', *International and Comparative Law Quarterly*, Vol. 45, 1996, pp. 162-177

4. D. Kritsiotis, "The Kosovo Crisis and NATO's Application of Armed Force against the Federal Republic of Yugoslavia", *International and Comparative Law Quarterly*, Vol. 49, 2000, pp. 330-359

5. Katz, "Issues Arising in the Icelandic Fisheries Case", *International and Comparative Law Quarterly*, Vol. 22, 1973, pp. 85-88

6. D W Greig, "Self-Defence and the Security Council: What does Article 51 Require", *International and Comparative Law Quarterly*, Vol. 40, 1991, pp. 366-402

7. C Greenwood, "Iraq's Invasion of Kuwait: Some Legal Issues", *World Today*, Vol. 47, 1991, pp. 39-43

8. White and McCoubrey, "International Law and the Use of Force in the Gulf", *International Relations*, Vol. , 1991, pp. 347-373

9. Anthony Aust, "The Procedure and Practice of the Security Council Today", pp. 365-374

10. Sir Anthony Parsons, "The Security Council an Uncertain Future", *Occasional Paper of the David Davies Memorial Institute of International Studies*, ISSN: 1353-9884, pp. 1-16

11. M N Shaw, *International Law* (Grotius: Cambridge, 1997) (4th edition)

Ms Ong Yen Nee is currently a Staff Officer in the Defence Policy Group. She graduated with a BA (Merit) in Political Science and Mathematics from NUS in 1997 and joined MINDEF as a Research Officer. She obtained a MA (Distinction) in International Studies and Diplomacy from the School of Oriental and African Studies, London in 2001.

Book Review:

Defence and Decolonisation in Southeast Asia: Britain, Malaya and Singapore 1941-68 (Richmond, Surrey: Curzon Press, 2001) by Karl Hack

Reviewd by LTA (NS) Toh Boon Ho

Studies on the British colonial empire in post-war Southeast Asia constitute a narrow historiography when judged against the voluminous output devoted to the Malayan Campaign and the Second World War in Southeast Asia. *Defence and Decolonisation in Southeast Asia: Britain, Malaya and Singapore 1941-68*, is one of the latest additions to the growing number of scholarly studies on post-war Southeast Asia, with a specific focus on Britain's strategic role in the region.

Hack's study covers the same period found in chapters 10 and 11 in *Between Two Oceans: A Military History of Singapore From First Settlement to Final British Withdrawal*.[1] Rather than rely on secondary sources only, Hack has made extensive use of declassified government records in the Commonwealth and the United States for his work. The end-result is an enlightened perspective on British colonial, defence and foreign policies in the Southeast Asian region.

Post-war British policy, Hack argues, hinged on the administrative consolidation of British colonial territories in the region in preparation for eventual self-determination along a carefully controlled programme designed for minimal disruption to long-term British interests. But with the onset of the Cold War less than five years after the end of the Second World War and the outbreak of the Malayan Emergency, British plans, so carefully planned and articulated in London during the wartime period, had to rapidly adapt to changed local circumstances through accommodation with willing local elites in the colonial territories.

The Malayan Emergency was, in Hack's view, a microcosm of British colonial management. Britain was able to exploit inter-ethnic and intra-ethnic differences to shape the decolonisation agenda. The largely Chinese nature of the insurgency ensured Malay support for the British counter-insurgency effort. Concurrently, Britain was careful not to alienate moderate Chinese opinion and endeavoured to broker an accommodation between moderate Chinese leaders and the Malay nationalist leadership. However, ethnic divisions within Malayan society were to prove a double-edged sword. British efforts to encourage the creation of a viable multi-ethnic political party failed to win popular support. While Britain was able to achieve a successful accommodation with the local Malay elite following the Malayan Union fiasco, it failed to achieve its ultimate goal of handing over power to a broad-based, multi-ethnic Malayan political party. It had to settle for a pro-Western, multi-ethnic but Malay-dominated coalition of communal political parties instead.

Besides coping with internal rebellion in Malaya, externally, Britain also had to contend with an unsettling regional background created from the collision of national self-determination and the re-imposition of colonial control. To the chagrin of British observers, the steadfast refusal of France and the Netherlands to arrive at any form of accommodation with local nationalist forces served to radicalise local anti-colonial forces. In the context of the Cold War, Britain relied on the support of her European allies in Europe against the Soviet menace. In Southeast Asia, drawing from the lessons of its humiliating defeat in 1942, she recognized that Malaya's defence lay with the greater region, and not just within its constituent borders.

On this premise, Britain placed a premium on regional security co-operation with France. The fall of Indochina to the new Communist menace, according to British assessments, would lead to a Communist re-enactment of the Japanese invasion of Southeast Asia in 1941-42.

Key to the security equation was Thailand's allegiance in future regional conflicts. Shaped by its bitter experience in 1942, Britain had cause to believe that Thailand would prove to be an unreliable ally and had strong reasons to doubt Thai resolve in a confrontation. Therefore, to safeguard Malaya's defence against a renewed external threat, the logical answer was the occupation of the Kra Isthmus. It was essentially, a re-working of the ill-starred Operation*Matador*. Yet, to draw the same historical parallel between British post-war and pre-war defence policy, Malaya, though valuable in peacetime, was deemed expendable in a global conflict. Plans were afoot for a Songkhla defence line, but no resources were allocated for the project. As Hack observes, "...as in 1941, there was a high chance of Songkhla plans being paralysed by political indecision in a crisis."[2] It was a dilemma that was never fully resolved.

A potential panacea lay with the nuclear option. In the 1957 Defence White Paper, London sought to realize cost savings and a credible deterrent in the form of the nuclear shield. In the Far East, plans and resources were devoted to the creation of a credible nuclear capability. Britain's nuclear role, together with the Commonwealth Strategic Reserve, was to be the Commonwealth's contribution to SEATO and the maintenance of regional stability. Singapore, as the key British defence base in the region, was equipped to handle such a role. [3]

But thermonuclear weaponry did not translate into cheap defence, nor was it effective against a low-intensity conflict scenario. The nuclear option did not stop Sukarno from proclaiming Confrontation between 1963-66. Britain, together with its Commonwealth allies, had to mount a protracted and expensive conventional defence of the newly created Malaysia against Indonesian aggression.[4] Britain was determined to maintain its great power status and retain its influence in the region, even at the expense of its military commitments in Europe.[5] Financial stringency, however, put paid to British pretensions. The strident expression "we must cut our coat according to our cloth" increasingly pervaded Whitehall's corridors from the mid-1960s onwards. On hindsight, Britain's victory in the Confrontation marked the highpoint, perhaps even the breakpoint, of British influence in Southeast Asia.[6]

The sterling crisis, on the other hand, marked the nadir of Britain's involvement in the region. British political and military leaders were determined to maintain the "East of Suez" posture. But Britain's global military commitments, principally in Southeast Asia, broke the bankliterally.[7] The end result was reluctant withdrawal and the restriction of Britain's military role to Europe after 1971.

Overall, Hack's work offers a good treatment of post-war British colonial, defence and foreign policies in Southeast Asia. The comprehensive treatment of the period 1945 to 1957 constitutes the strength of this book. But Hack's account of the post-1957 period is best supplemented by other accounts cited in the endnotes to gain a fuller picture of the strategic conundrum faced by British policy-makers.

*The abovementioned title is available for borrowing at the **SAFTI MI Library**. The catalog references are:*

Defence and Decolonisation in Southeast Asia : Britain , Malaya and Singapore 1941-68
Karl Hack
DS596.3 HAC

Endnotes

1 See author's book review of *Between Two Oceans: A Military History of Singapore From First Settlement to Final British Withdrawal* (Singapore: Oxford University Press, 1999) in *Pointer*, 26, 1 (January - March 2000), pp. 114-117.

2 Karl Hack, *Defence and Decolonisation in Southeast Asia: Britain, Malaya and Singapore 1941-68*(Richmond, Surrey: Curzon Press, 2001), p. 92.

3 Ibid., pp. 210, 243. See also Richard Moore, "Where Her Majesty's Weapons Were", *Bulletin of Atomic Scientists*, 57, 1 (January/February 2001), pp. 58-64.

4 See author's book review of *The Undeclared War: The Story of the Indonesian Confrontation 1962-1966*(Singapore: Donald Moore, 1971) in *Pointer*, 27, 1 (January March 2001), pp. 133-136.

5 Michael Middeke, "Global Military Role, Conventional Defence and Anglo-American Interdependence afterNassau", *Journal of Strategic Studies*, 24, 1 (March 2001), pp. 143-164.

6 Recent studies indicate that by 1965, Britain was at the end of its tether. The financial costs of military operations in Borneo were ruining its balance of payments. Had Sukarno not been replaced by the moderate Suharto who ended the conflict, Britain would have to truncate its responsibilities prematurely. For a good account, see John Subritzky, *Confronting Sukarno: British, American, Australian and New Zealand Diplomacy in the Malaysian-Indonesian Confrontation, 1961-5* (London: Macmillan Press Ltd., 2000).

7 In spite of US efforts, bordering on veiled threats at times, to compel Britain to maintain its role in Southeast Asia in line with American involvement in Vietnam, and US attempts to shore up the pound, Britain ultimately capitulated to financial reality. See Diane B. Kunz, "'Somewhat Mixed Up Together': Anglo-American Defence and Financial Policy during the 1960s", in *The Statecraft of British Imperialism: Essays in Honour of Wm. Roger Louis*, ed. Robert D. King and Robin W. Kilson (London: Frank Cass, 1999), pp. 213-232.

Personality Profile:

Mohammad Ali Jinnah

Revered by Pakistanis as their Quaid-e-Azam, the Great Leader and Father of the Nation, Mohammad Ali Jinnah, alongside Mahatma Gandhi and Jawaharlal Nehru, was a pivotal figure in the Indian subcontinent's decolonisation. Ironically, the pursuit of freedom and self-determination also resulted in the partition of British India into Pakistan and India. The strategic and security repercussions of partition continue to haunt Indo-Pakistani relations.

Jinnah was born on 25 December 1876 into a prominent merchant family in Karachi. When he reached 16, his father sent him to London to be apprenticed to Graham's Trading Company. It was hoped that the young Jinnah would gain the necessary skills and experience to take over the business in the future. However, in 1893, the headstrong young man decided to pursue a career as a barrister where he would be independent. He was also inspired by how the great contemporary and past leaders of Britain had been trained in the law. Jinnah joined Lincoln's Inn and, in 1896, became the youngest Indian to be called to the Bar. Jinnah's sister later claimed that it was his varied experiences in London which caused him to become "an uncompromising enemy of all forms of colour bar and racial prejudice."

On his return to India, he set up his practice in Bombay (now Mumbai) and became a very successful lawyer. Firmly established in the legal profession, Jinnah formally joined the Indian National Congress in 1905, thus making his debut in politics. He served together with senior Indian advocates of self-government such as Gopal Krishna Gokhale and Dadabhai Noaroji. Jinnah was also the first parliamentarian to have a Private Member's Bill passed at the Imperial Legislative Council of India.

Jinnah was hailed as the leading ambassador of Hindu-Muslim unity with the conclusion of the Lucknow Pact in 1916. He had invited the All-India Muslim League to hold its annual session in Bombay simultaneously with that of the Congress. He acted as the principal conciliator between Congress and the Muslim League, bridging the differences and ensuring its successful adoption. The Pact represented a compromise between the Congress and the Muslim League on Muslim claims in a post-war democratic constitution. This allowed the two organisations to present the British with an effective united front of the Home Rule League. Thus the Lucknow Pact became the basis for the Montagu-Chelmsford Reforms, also known as the Act of 1919.

Jinnah's pragmatic stance can be seen from his speech at Lucknow when he said: "In the affairs of our common secular existence, we have to deal not with angels but with men, with passions, prejudices, personal idiosyncrasies, innumerable cross-currents of motive, of desire, hope, fear and hate. The Indian problem has all such formidable complications in its texture." He emphasised that the Muslim community must have its own self-respect, saying: "We want no favours, and crave no partial treatment. That is demoralising to the community and injurious to the State. The Muslims must learn to have self-respect. What we want is a healthy and fair impetus to be given to our aspirations and ideals as a community."

Jinnah had also been associated with gradual change through constitutional methods. He had been influential in getting the Muslim League to declare, in 1913, that its objective was: "Attainment under the aegis of the British Crown of a system of self-government suitable to India through constitutional means, by bringing about a steady reform of the existing system of administration, by promoting a steady national unity, by fostering public spirit, and by cooperation with other communities for the said purpose." Thus Jinnah was dismayed when Gandhi, who had been elected to the presidency of the Home Rule League in 1920, embarked on a path of *satyagraha* (civil disobedience) and invocation of Hindu religious motifs in order to secure *swaraj* (self-rule) within the unrealistic time frame of a year. He felt that Gandhi's methods were extra-constitutional. He also feared the injection of religion into politics was a mistake as it would distract Hindus and Muslims from their common political cause and principles. Anti-government demonstrations often turned into communal riots with many deaths in places like Malabar and Chuari Chuari. By then, Jinnah had resigned from Congress and the Home Rule League.

The Nehru Report, released in 1928 as the Congress' proposals for the future constitution of India, was a source of friction between the Hindu and Muslim communities. It negated the main points of the Lucknow Pact and did not take into the account the proposed concessions of the 1927 Delhi Muslim Proposals. The Nehru Report's blanket refusal of even minimal Muslim demands dealt a severe blow to Jinnah's efforts to bring about Hindu-Muslim unity. A friend later recounted how it was "the last straw" and "the parting of ways" for Jinnah. In the early 1930s, his disillusionment with Indian politics caused him to move to London in a form of self-imposed exile. He later recounted: "Not that I did not love India, but I felt utterly hopeless."

However, the pleadings of his followers convinced Jinnah to return in 1935. He revived the decaying branches and provincial organisations of the Muslim League. He also tried to rally provincial Muslim leaders to sink their differences and fight for the rights of their community, rather than their private interests, under the banner of the Muslim League.

In the 1937 elections, the Congress came to power exclusively in seven out of 11 provinces. The predominantly Hindu program of the Congress governments caused Muslims to fear that their religion, language and culture were not safe and that they could live only at the sufferance of Hindus and as second class citizens. Jinnah seized upon this groundswell to forge the Muslim League into a truly all-India, mass-based organisation. Until then, Congress tended to see Jinnah and the Muslim League as representing only the Muslim upper middle classes especially since Jinnah was more comfortable speaking English than the Muslim *lingua franca* of Urdu.

By 1940, Jinnah had become the undisputed leader of Muslims in India. He had become convinced that a partition of India along religious lines was the only way to preserve Muslim political power and culture. He declared that the Muslims of India were a separate nation and were entitled to a separate state. That year, the Muslim League adopted the Lahore Resolution calling for a separate autonomous state in the majority-Muslim areas of northeastern and eastern India the demand for Pakistan.

This demand was fiercely resisted by Congress. The British were opposed as well as they felt that their greatest legacy to the Indian people would be a united India. Attempts to negotiate with the Muslim League on the basis of the Cripps offer and Rajaji formula, which might have satisfied Jinnah in 1928, were rejected as offering only a "moth-eaten, mutilated" Pakistan, appended with too many conditions. Another attempt at preserving unity was made with the high level Cabinet Mission Plan of 1946. It stipulated a limited centre, having authority only over foreign affairs, defence and communications. It would consist three autonomous groups of provinces - the northeastern and eastern groups would be Muslim-controlled while the mainland would be Hindu-dominated. Jinnah was to accept this in principle, only to rescind it after perceived obstructionism and defiance from Congress, which Jinnah claimed was designed to browbeat the Muslim League into accepting Congress' dictates and interpretations of the plan. Jinnah called for demonstrations to oppose the formation of an interim Indian government and renewed his demand for partition. Communal riots erupted resulting in more than 3,000 killed and thousands wounded.

Lord Mountbatten, the new Viceroy was unable to dissuade Jinnah and partition was agreed to on 3 June 1947 by the Congress, Muslim League and Akali Dal (representing the Sikhs). The British thus handed over

power to two successor states on 15 Aug 1947. Jinnah was to be Governor-General of East and West Pakistan. But to almost 100 million Pakistanis, their Quiad-e-Azam was more than a Governor-General. He worked to consolidate the new state which started without a central government, capital or organised defence force. The treasury was empty as India held its sterling balances initially. Rioting had devastated much of the Punjab and disrupted communications. The exodus of the Hindu and Sikh business and managerial classes also left the economy in an extremely difficult situation. In addition, India annexed Junagadh and war erupted over Kashmir from October 1947 to December 1948. Only Jinnah's charismatic leadership and ability played a large role in holding the fledging state together. Eventually the strain of exhaustion from over-work, poor health and tuberculosis caused Jinnah's death on 11 September 1948, only 13 months after Pakistan's creation.

Critics of Jinnah have portrayed him as a cold megalomaniac who demanded for a separate Pakistan for the sake of his own political ambition. His successors have disputed the degree to which he was committed to secular government. Two further wars over Kashmir were fought in 1965 and 1971. East Pakistan, with the help of Indian military intervention, broke away to form the independent state of Bangladesh. However one may judge Jinnah and his legacy, he remains one of the giants of the modern history of the Indian subcontinent.

Bibliography

Hamid Jalal et al, *Pakistan: Past & Present* (London: Stacey International, 1977).

Khalid Bin Sayeed, *Pakistan: The Formative Phase 1857-1948*

(Karachi: Oxford University Press, 1968)

Selected Books and Reports:

Henry A. Kissinger

Henry A. Kissinger attended George Washington High School in New York and later went to Harvard where he obtained his Ph.D. He taught government and international affairs at Harvard from 1957 to 1969. At various times he has also been a consultant to several governmental boards and agencies including the National Security Council, the United States Arm Control and Disarmament Agency, and the Weapons Systems Evaluation Group of the Joint Chiefs of Staff. At the height of his career, he served as Secretary of State under Presidents Nixon and Ford from 1973 to 1977.

Dr. Kissinger has written many books and articles on politics, defence and international affairs and is widely acknowledged and honoured for his public and international service. He was the recipient of the1973 Nobel Peace Prize as well as the 1977 Presidential Medal of Freedom.

Nuclear Weapons and Foreign Policy (1957) is one of Kissinger's earlier and better known books. It received the 1958 Woodrow Wilson Award which is given out annually to honour outstanding books in the fields of government and international politics. It was also awarded a citation by the Overseas Press Club. In this book, the author discusses the challenges, the dilemmas and the impact of the coming of the nuclear age. Written when the nuclear age was in its infancy, when rules were unclear and when a nuclear war seemed so dangerously imminent, Kissinger provides the details, the rules and the description of the after-effects of a nuclear war in his book. An abridged version was published in 1969.

Dr. Kissinger published *The Necessity for Choice* (1961) in an attempt to define defence and foreign policy issues that confronted America then. In the book, Dr. Kissinger shares his conviction that established patterns of policy will no longer hold true, that in the age of revolution, the choice is for Americans to face the challenge of change and risk, and for America as a nation to overcome its need for safety and predictability.

In his book, *The Troubled Partnership* (1965), Henry Kissinger critically examines the whole future of the Atlantic Community. With characteristic incisiveness, he examines the causes of the strains in the alliance and presents his views on how the future of NATO can only be shaped by changes in US political and military attitudes.

Dr. Henry Kissinger published *For the Record: Selected Statements* (1977) after his retirement as Secretary of State, and in it, he tackles a wide range of issues such as the future of NATO, the SALT II treaty, human rights and American policy, Middle East policy and the future of international business amongst many others.

Dr Kissinger served as an assistant to the President for National Security Affairs from January 1969 to January 1973. *White House Years* (1979) captures most of the momentous happenings during his term as the assistant to the President. The book was awarded the 1979 American Book Award in History. In this book, Dr. Kissinger speaks of his first meeting with then President Nixon, his secret trip to China, the first Strategic Arms Limitation Treaty (SALT) negotiation, the Jordan crisis of 1970, the India-Pakistan war of 1971, the historic summit meetings in Peking and Moscow, the major controversies over Indochina policy and other highlights.

Years of Upheaval (1982) is a recollection by Dr. Kissinger of the turbulent years of the second Administration of President Nixon when he served as the Secretary of State. It is a vivid and rich account of momentous events such as the Watergate Scandal and the 1973 October war in the Middle East. Dr. Kissinger's frank account of President Nixon's last days, appraisals of other world leaders and insights into the nature of diplomacy and political leadership, make this book a fascinating read.

Diplomacy (1994) is a sweeping overview of the history of diplomacy by the Western Great Powers. Dr. Kissinger traces the political and diplomatic manoeuvring which surrounded major international events like the First World War, the inter-war period, the Second World War, the Cold War and the beginning of the "New World Order". One of his major underlying claims is how American power and dominance brings order and stability to the international system.

The Kissinger Transcripts (1999) provides a candid and explicit record of formerly classified "Top Secret" information relating to Dr. Kissinger's talks with top political figures, such as Richard Nixon, Leonid Brezhnev, Mao Zedong, Deng Xiaoping and George Bush, among others. These transcripts show how Dr. Kissinger conducted his diplomatic manoeuvres with China and the Soviet Union and give readers an insight into how American diplomacy is conducted by one of its protagonists. His experience in the foreign policy arena bequeathed upon him many longstanding friendships. A hint of that can be discerned from the foreword that he contributed to the second volume of Senior Minister Lee Kuan Yew's memoirs, *From Third World to First* (2000).

Dr. Kissinger has not always been on the winning side of history, especially with respect to Vietnam. However his eloquence and prolific output will, no doubt, help to shape how we read the historical record and his place in it.

The above books are available at the SAFTI Library.